El círculo virtuoso para la Protección de Datos Personales: Legislación, control y responsabilidad social empresaria.[1]

Dra. María Laura Spina[2]; Marcelo G. I. Temperini[3]

Abstract en Español. La República Argentina posee a nivel nacional una legislación constitucional y legal sobre habeas data buena y suficiente, pero para su efectiva protección debe concretarse el armado de la Red Argentina de Protección de Datos Personales por parte de los Estados Provinciales. Para ello, debe regularse las cuestiones que le son propias en materia de procedimiento y control, de manera armónica tanto por razones de coordinación como seguridad jurídica. En la Sociedad de la Información, además del cumplimiento de las normas jurídicas aplicables, las empresas y corporaciones, privadas y públicas, deben tener un comportamiento ético sobre los datos personales que manejan por razones de responsabilidad social.

Abstract en Inglés: The Republic of Argentina has a national legal and constitutional law on habeas data good enough, but for their effective protection must specify the assembly of the Red Argentina Personal Data Protection by the Provincial States. This should be regulated the issues which are peculiar procedural and control, so harmoniously both for reasons of coordination and legal certainty. In the Information Society as well as compliance with applicable legal standards, companies and corporations, private and public, ethical behavior should be on that handle personal data for reasons of social responsibility.

Keywords: Protección de datos personales – habeas data - ética de la información - responsabilidad social empresaria – RSE - competencia provincial - competencia federal – ley provincial de adhesión – Constitución Provincial – Constitución Nacional

---

[1] El presente trabajo se enmarca dentro del Plan de Investigación de "La Protección de Datos Personales como Responsabilidad Social Empresaria en las Pequeñas y Medianas Empresas de la ciudad de Santa Fe", el que depende del Proyecto de Investigación y Desarrollo CAI+D titulado "Gobierno Corporativo y Responsabilidad Social Empresaria, acreditado por la Secretaría de Ciencia y Técnica de la Facultad de Derecho y Ciencias Sociales, de la Universidad Nacional del Litoral.

[2] Abogada (UNL), Magister en Ciencias de la Legislación, Profesora adjunta a cargo de la cátedra Derecho y Tecnologías de la Información. estudiojuridicospina@gmail.com

[3] Director de la Red Iberoamericana de Derecho Informático – elderechoinformatico.com, Estudiante de Derecho de FCJS de UNL. Cientibecario UNL Convocatoria 2010 e integrante de CAID "Gobierno Corporativo y Responsabilidad Social Empresaria". temperinimarcelo@gmail.com

Introducción.

En la actualidad, la información es un activo imprescindible en todas las organizaciones, y su importancia está presente en todos los ámbitos de actividad.

Los datos personales son una de las más habituales y principales especies de información, las empresas y organizaciones, utilizan a diario sus bases y registros de clientes, proveedores, empleados, pacientes, consumidores, de marketing, de concursos o sorteos, etc.

El desarrollo acelerado que tienen las "redes sociales" y la utilización que hace el mercado de ellas, hace necesario optimizar los mecanismos de protección de los datos personales y prestar atención a los aspectos inconclusos de este subsistema jurídico.

El objeto de este trabajo es hacer un repaso y actualización sobre la situación de la protección de datos personales en Argentina, respondiendo a algunos interrogantes y dando algunas recomendaciones básicas para intentar armonizar y coordinar las diferentes regulaciones que existen en el territorio de nuestro país.

El plexo normativo de Argentina en materia de datos personales, es uno de los más avanzados de América Latina. Sin embargo, presenta características diversas y complejas, en el juego de las materias delegadas y los poderes reservados constitucionalmente entre las Provincias y la Nación.

El derecho de Habeas Data fue incorporado por la reforma de 1994 en el art. 43 de Constitución Nacional Argentina, y fue regulado a partir del año 2000 por la ley nacional Nº 25.326. Casi todo el contenido de esta norma tiene alcance de orden público, pero una parte sólo tiene ámbito de aplicación federal y las provincias conservan sus atribuciones originarias legislativas, por lo cual deben reglamentar determinados procedimientos y controles.

Todavía es escaso, en general, el marco de regulación que han establecido las provincias, del cual haremos más adelante un análisis detallado hasta el 1º de mayo de 2010.

Es necesario destacar que, más allá de las regulaciones estatales, es posible hacer mejor las cosas, por el bien de los demás, en materia de protección de datos personales dentro de los estándares internacionales de responsabilidad empresaria, gubernamental y corporativa.[4]

Recordemos el concepto de la Responsabilidad Social Empresaria (RSE): podemos decir que es un modelo de gestión ética integral que permite un cambio interno y externo donde se desenvuelve la empresa[5] .

En la ética de la información uno los principios que nos trae Stiglitz[6] para la economía internacional es: "No aprovecharse de la Información. Ser transparente".

En materia de datos personales, la RSE puede tener varias aplicaciones, por ejemplo dentro del ámbito de los derechos del consumidor, de las redes sociales (fundamentalmente en relación a los niños) y los datos críticos o sensibles, que son aquellos de más riesgo y en los que se deben extremar las precauciones, por nombrar algunos casos típicos.

[4] Familia de Normas ISO-IEC 27000 (SGSI). En elaboración normas ISO 26.000 de RSE.

[5] Nicolás Liarte-Vejrup y Marcos Zuazaga. La Responsabilidad Social Empresaria de los productores agropecuarios con su público interno.

[6] Joseph E. Stiglitz. Ética, Asesoría Económica y Política Económica.

Debemos como operadores del Derecho atender a lo jurídico, pero recomendando a nuestros clientes comportamientos éticos y buenas prácticas en relación al uso de las TIC's ya que en el mundo interconectado los escándalos y las condenas sociales pueden ser tanto o más gravosas que las judiciales.

Ámbito de Aplicación

La ley de protección de datos personales, Nº 25.326, al definir en su artículo 44 su Ámbito de Aplicación[7] dice que las normas de los Capítulos I, II, III y IV y el art. 32 son de orden público y de aplicación en lo pertinente en todo el territorio nacional. De su texto, queda claro que los capítulos no señalados expresamente, no son de aplicación nacional y que deben ser regulados por las Provincias. Es decir, son de orden público los Capítulos de: Disposiciones Generales; Principios generales relativos a la protección de datos, Derechos de los titulares de los datos, Usuarios y responsables de archivos, registros y bancos de datos; y el artículo 32, que en realidad incorpora 2 delitos penales al Código Penal (más precisamente el 117 bis y 157 bis, luego reformados con la Ley Nº 26.388 del año 2008).

Fig. 1.

Ámbito de Aplicación Territorial de la Ley Nº 25.326 (Art. 44)		
Materia	**Aplicable en todo el territorio nacional (orden público)**	**No aplicables en todo el territorio nacional**
Capítulo I: Disposiciones generales	SI	NO
Capítulo II: Principios generales relativos a la protección de datos	SI	NO
Capítulo III: Derechos de los titulares de datos	SI	NO
Capítulo IV: (Obligaciones de los) usuarios y responsables de archivos, registros y bancos de datos	SI	NO
Capítulo V: Órgano de control	NO	SI
Capítulo VI: Sanciones (que puede imponer el órgano de control)	NO	SI
Capítulo VII: Acción de protección de los datos personales (habeas data): Procedimiento aplicable	NO	SI
Art. 32: Sanciones penales	SI	NO
Art. 44: Archivos, bases y registros interconectados a nivel interprovincial, nacional o internacional	SI	NO

[7] ARTICULO 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.

Queda entonces en el ámbito Provincial, los Capítulos de: Sanción, Control y Acción de Protección de los datos personales. Creemos que esto ha sido un acierto, ya que de lo contrario se estaría incurriendo en la vulneración de competencias provinciales, sea por materias procesales (como en el caso de regulación de la acción de protección de datos personales), o por materias de policía (en el caso de control y sanción).

Siguiendo con el art. 44 de la Ley Nº 25.326, en el segundo párrafo, corroborando la interpretación del primero, la ley invita a las provincias a adherir a las normas que fueren de exclusiva aplicación en el ámbito nacional, confirmando nuevamente que los Capítulos V, VI y VII son competencia de las legislaturas provinciales.

En igual sentido, cuando La Comunidad Europea analizó la situación del contexto jurídico argentino en la Decisión de fecha 30/06/2003 afirmó que "Determinadas normas de la Ley son aplicables de manera uniforme en todo el territorio argentino: disposiciones generales y disposiciones sobre los principios generales relativos a la protección de datos, derechos de los titulares de datos, obligaciones de los usuarios y responsables de archivos, registros y bancos de datos, sanciones penales, así como la existencia y características principales del recurso judicial habeas data tal como se establece en la Constitución." [8]

Otras disposiciones de la Ley son aplicables a los registros, archivos y bases o bancos de datos interconectados en red a nivel interjurisdiccional (es decir, interprovincial), nacional o internacional, y se considera que competen a la jurisdicción federal. Dichas disposiciones hacen referencia al control ejercido por el órgano de control, las sanciones impuestas por el órgano de control y el procedimiento aplicable en caso de recurso judicial habeas data. **En cuanto a otros tipos de archivos, registros y bases de datos, debe considerarse que competen a la jurisdicción provincial y que las provincias pueden legislar al respecto**". [9]-[10]

Esta decisión, fue basada en el Dictamen 4/2002 sobre el nivel de protección de datos personales en Argentina, adoptado el 3 de Octubre de 2002, por el Grupo de Trabajo sobre Protección de Datos, que es un órgano consultivo independiente de la Unión Europea sobre protección de datos, creado por el art. 29 de la Directiva 95/46/CE. Este Dictamen, ha desarrollado de manera minuciosa y precisa el estado de la protección de datos personales en nuestro país, que si bien se realizó en Octubre del 2002, casi 8 años después el estado es prácticamente igual (salvo algunas nuevas disposiciones de la D.N.P.D.P., que no vienen a cambiar el panorama general).

Habeas Data en las Constituciones Provinciales.

A continuación desarrollaremos un cuadro de análisis y comparación de Constituciones Provinciales y Ciudad Autónoma de Buenos Aires (CABA) donde se ha encontrado referencia sobre la regulación del derecho a los datos personales. En el mismo se ha intentado encontrar elementos comunes a todas las regulaciones, con el

[8] Decisión de la Comisión, 30/06/2003, Comisión de las Comunidades Europeas, Inciso 11.
[9] Decisión de la Comisión, 30/06/2003, Comisión de las Comunidades Europeas, Inciso 12.
[10] El resaltado es de los autores

fin de poder sistematizar un cuadro comparativo. Las Provincias que no se señalan en el cuadro es porque no se les ha encontrado (hasta la fecha) regulación alguna sobre habeas data.

Fig. 2. Análisis y Comparación de las Constituciones Provinciales

Provincia		Constitución (Arts.)	Caractéres						Observaciones
			A	B	C	D	E	F	
	Chaco	Art. 19							-
	Chubut	Art. 56							-
	Córdoba	Art. 50							Sólo garantiza el derecho de acceso, actualización y rectificación (falta supresión y confidencialidad)
	Entre Ríos	Art. 63							Amplía el derecho de acceso a datos del titular, Restringe el derecho de supresión o confidencialidad a los datos sensibles
	Jujuy	Art. 23 inc. 6, 7 y 8							Sólo garantiza el derecho de acceso y rectificación.
	La Rioja	Art. 28 bis y 30							Menciona la garantía al derecho de autodeterminación informatica (doctrina europea)
	Neuquén	Art. 61							
	Río Negro	Art. 20							Es un artículo que asegura la intimidad de las personas.
	Salta	Art. 89							
	San Juan	Art. 26							Prohíbe tratamiento datos sensibles, salvo disociación de datos.
	San Luis	Art. 21							Art. sobre libertad de expresión y derecho a la información. Incorpora el derecho a réplica y garantiza sólo el derecho de acceso.
	Santiago del Estero	Art. 60							-
	Tierra del Fuego y Antártida	Art. 45							-
	Provincia de Buenos Aires	Art. 20 3er párrafo							Si bien menciona que debe ser regulado por ley, afirma que es una garantía operativa.

Referencias Figura Nº 2 Análisis y Comparación de Constituciones Provinciales

A) Redacción básica (similar al art. 43 3er párrafo de la CN.).
B) Prohibición de fines discriminatorios.
C) Sin limitación de derechos (modificación, actualización, supresión y confidencialidad).
D) Sin discriminación de tipos de Bases .
E) Acceso por parte de terceros (con interés legítimo).
F) Uso de la Informática sin vulnerar honor e intimidad.

A) Redacción básica: En este elemento, se considera que la redacción del artículo es igual o similar a la redacción original del derecho de Habeas Data en la Constitución Nacional (Art. 43, 3er párrafo). También se aplica a aquellos artículos

que si bien la redacción no sigue la misma estructura y orden, contiene todos o la mayoría de sus elementos[11].

B) Prohibición de Fines Discriminatorios: Elemento extra, inserto expresamente en algunos artículos constitucionales, en el cuál se prohíbe todo uso o tratamiento de datos personales con fines discriminatorios. Vale destacar que si bien este elemento no se encuentra expreso en la redacción original de Habeas Data de nuestra Constitución Nacional, en la posterior Ley 25.326 de Protección de Datos Personales, en el art. 3, 2do párrafo, reza que "Los archivos de datos no pueden tener finalidades contrarias a las leyes o a la moral pública", y dentro de este espectro bien podría considerarse que los fines discriminatorios están prohibidos, consideramos positivo su inclusión expresa en el artículo, fortaleciendo el espíritu propio del derecho, que es precisamente la de proteger el honor y la intimidad de las personas.

C) Sin limitación de Derechos: La consideración de este elemento dentro del artículo de Habeas Data, supone no un elemento extra, sino una modificación a uno de los elementos de la redacción original (elemento 4). En nuestra Constitución Nacional, los derechos de supresión, rectificación, confidencialidad o actualización son a condición de que exista falsedad o discriminación. Consideramos que esta fórmula es más precisa para el caso de la persona que desea ejercitar sus derechos frente a un registro de datos público o legal, donde debe existir alguna de estas circunstancias para poder brindar estos derechos. Dicho requisito, se vuelve a repetir, incluso con mayor énfasis en la Ley 25.326, Art. 38, 2do párrafo, donde entre los requisitos de la demanda (de la acción de protección de datos personales), se exige incluir por escrito "los motivos por los cuales considera que la información que le atañe resulta discriminatoria, falsa o inexacta".

Ahora, en el caso de que sean bases de datos privadas, dichas limitaciones no son exactas, ya que dicha redacción estaría prohibiendo (por ejemplo) a un titular de datos, exigir que el responsable de un determinado registro de datos privados, lo suprima de dicha base, o bien guarde confidencialidad del mismo. En dichos casos el hecho de exigir que dichos datos sean falsos, inexactos o discriminatorios al titular, estaría suponiendo una limitación infundada a su derecho.

Con estos fundamentos, es que consideramos más adecuado, en principio, no limitar el ejercicio de los derechos (tal como sucede en algunas constituciones provinciales).

D) Tipos de Bases: Este carácter, es una modificación al elemento 3 de la redacción original, ya que evita la clasificación realizada entre registros y bancos de datos públicos, y los privados destinados a proveer informes. En la misma, ahora sólo se menciona a los registros o bases en formal general. Consideramos que dicha modificación es positiva, dado que la clasificación del artículo original, ha traído conflictos e inconvenientes de interpretación, por aquellos poseedores de bases de datos privadas, que consideraban que "no eran destinadas a proveer informes", por lo tanto, dichas obligaciones no le eran aplicables. Luego de algunos fallos aclaratorios,

[11] Constitución Nacional Art. 43, 3er párrafo: *Toda persona (1) podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad (2), que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes (3), y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos (4). No podrá afectarse el secreto de las fuentes de información periodística (5).*

hoy en día es un tema que se encuentra saldado, considerando que las obligaciones corren para todas las bases, excepto aquellas de uso personal y privado (como las agendas telefónicas, etc.). Por todo lo dicho, consideramos positiva la modificación de este elemento.

E) Acceso por parte de terceros: Este carácter supone el agregado de un elemento extra a la redacción original. En el mismo, se considera la prohibición de que terceros accedan a los datos personales de una persona, a excepción de que posean algún interés legítimo, o bien haciendo referencias a casos excepciones regulados por la ley. Si bien dicho elemento no se encuentra en el Habeas Data de la Constitución Nacional, sí se encuentra de cierta manera en la regulación proporcionada por la Ley 25.326, donde en el art. 34, sobre legitimación activa de aquellos que pueden interponer la acción de protección de datos personales, aparte del titular, se menciona a sus tutores o curadores y los sucesores de las personas físicas, sean en línea directa o colateral hasta el segundo grado, por sí o por intermedio de apoderado. Con la fórmula utilizada de interés legítimo dentro de la excepción, quedaría desde nuestro punto de vista, un espectro más amplio de legitimados activos para poder ejercer el derecho. Consideramos que la inclusión de este elemento en los artículos provinciales de Habeas Data, es innecesario, ya que es una cuestión secundaria que bien puede ser regulada por su ley correspondiente.

F) Uso de Informática: Este carácter supone el agregado de un elemento extra a la redacción original. En el mismo, cuyo texto completo es "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", se agrega sin lugar a dudas un elemento de protección a la intimidad y honor de las personas más amplio que la propia protección de los datos personales, ya que consideraría toda otra afectación a estos derechos que pudiera realizarse mediante algún tipo de utilización de la informática.

¿Es necesario que los Estados Provinciales incorporen en sus textos constitucionales el Derecho de Habeas Data?

Las provincias adhieren a los derechos reconocidos por la Constitución Nacional, los cuales además son operativos, por lo cual no es indispensable que incorporen el Derecho de Habeas Data en sus textos constitucionales. No obstante, **aconsejamos su incorporación**, a los fines de un mayor compromiso y protección por parte de las Provincias, ocasión en la cuál es una oportunidad inmejorable para reparar algunos defectos legislativos que están plasmados en el texto de la Carta Magna.

Como se puede observar en la Figura Nº 2 un poco más de la mitad de las Provincias en mayor o menos medida han incorporado en sus normas fundamentales, el Derecho de Protección de Datos Personales (Habeas Data). De las 24 Jurisdicciones (23 Provincias más la Ciudad Autónoma de Buenos Aires) que tiene la República Argentina, 10 de ellas (en estadística, un 41,6% considerando un total de 24) no han trabajado de manera alguna el derecho a los datos personales.

En referencia al estudio realizado sobre la incorporación en los textos constitucionales, en las 14 Provincias donde se ha encontrado regulación en materia de datos personales, se podría realizar una clasificación en 2 niveles:

Regulación Avanzada: En este caso se consideran aquellas Provincias que han sabido regular el Derecho a los Datos Personales de la manera más adecuada según nuestra visión, ya sea por la corrección de algunos detalles del derecho (carácter C o D del cuadro de análisis) o bien porque a la regulación básica, le han agregado elementos (caracteres B, E o F)que brindan una mejor o más integral protección de la intimidad y el honor de las personas, fin último de la protección de los datos personales. Entre ellas, se podría mencionar a: Córdoba, Tierra del Fuego, Chaco, Buenos Aires (Provincia), y San Juan. (5/14)

Regulación Básica: En este caso se consideran aquellas Provincias que han regulado el Derecho a los Datos Personales de manera similar a la Constitución Nacional, con algunas diferencias quizás, pero que no consiguen mejorar su nivel de regulación. Entre ellas, se podría mencionar a: Chubut, Entre Ríos, Jujuy, La Rioja, Salta, Santiago del Estero, San Luis y Río Negro. (8/14).

Habeas Data en las Legislaciones Provinciales

A continuación desarrollaremos un cuadro de análisis y comparación de las Legislaciones Provinciales donde se ha encontrado referencia sobre la regulación del derecho a los datos personales, ya sea en cuanto a procedimiento (acción de habeas data) o cuestiones específicas sobre la materia. En el mismo modo que el cuadro anterior, se ha intentado encontrar elementos comunes a todas las regulaciones, con el fin de poder sistematizar un cuadro comparativo. Las Provincias que no se señalan en el cuadro es porque no se les ha encontrado (hasta el 1º de Mayo de 2010) regulación alguna sobre la acción de habeas data o sobre el tratamiento de datos personales.

Referencias a la Figura Nº3: Análisis y Comparación de Legislaciones Provinciales
A) Regula procedimiento de acción de datos personales (habeas data).
B) Adhiere al Régimen Nacional de Protección de Datos Personales (Ley Nº 25326).
C) Crea o designa un Órgano de Aplicación de la Ley.
D) Crea o designa un Registro de Datos Personales.
E) Regula funciones de sanción y control.
F) Incorpora el Habeas Data o alguna materia relativa a la protección del honor y la intimidad de las personas.
G) Regula la protección de datos personales (Simil Ley Nº 25326).

Fig. 3. Análisis y comparación de las Legislaciones Provinciales.

Provincia		Legislación	Caractéres							Resumen / Observaciones
			A	B	C	D	E	F	G	
	Chubut	Ley Nº 4244 (1996)	■							Ley de Habeas Data. Regula el procedimiento de la acción de habeas data, sin entrar en más detalles sobre la protección de datos personales.
	Córdoba	Ley Nº 9380 (2007)						■		Ley de Videovigilancia. Regula la instalación y utilización de cámaras por las fuerzas de seguridad pública, para contribuir a la investigación y prevención de contravenciones y delitos.
	Misiones	Ley Nº 3794 (2001)	■		■		■			En el art. 21, cuando designa el Órgano de Control, afirma que le compete al mismo la creación de un Registro Provincial.
	Neuquén	Ley Nº 2307 (2000)	■							Regulación Procesal de la Acción de Habeas Data.
		Ley Nº 2399 (2002)		■						En el art. 2, dice que el PE designará al organismo que actuará como autoridad de aplicación de la ley.
		Decreto 313/03			■	■	■			Se crea el Registro Provincial de Datos Personales (REPRODAP).
	Santiago del Estero	Ley Nº 6296 (1996)	■					■		Es un Ley de Amparo, que incorpora el habeas data y regula el procedimiento del amparo general.
	Tucumán	Ley Nº 6944 (1999)	■					■		Incorpora al Código Procesal Constitucional de Tucumán, en el Capítulo IV, de Amparos Especiales, el art. 67, de Amparo Informativo (Habeas Data).
	Mendoza	Ley Nº 7261 (2004)				■			■	Crea el Registro de Empresas Privadas de Información de Deudores (REPID). La ley regula el habeas data de forma similar a la Ley Nº 25326, pero con una orientación a las bases de datos financieras (riesgo comercial)
	Ciudad Autónoma de Buenos Aires	Ley Nº 104 (1998)							■	Regula el Acceso a la Información Pública.
		Ley Nº 1845 (2005)	■		■		■	■	■	Designa a la Defensoría del Pueblo de la Ciudad de Buenos Aires como órgano de control. En el art. 39, regula el uso del correo electrónico en el ámbito laboral.
		Disp. 119/2007				■	■			La Defensoría del Pueblo de la Ciudad de Buenos Aires crea el Centro de Protección de Datos Personales, el cuál tiene a cargo el Registro de Banco de Datos Personales del Sector Público.
		Ley Nº 2014 (2006)							■	Crea y regula el Registro No Llame.

¿Deben los Estados Provinciales adherirse al régimen Nacional de Protección de Datos Personales (Ley Nº 25.326)?

Reiteramos que la parte general de la Ley Nº 25.326 está plenamente vigente, y que no necesita adhesión, puesto que su articulado es considerado de orden público y por lo tanto, obligatorio en todo el territorio argentino[12]. Pero es necesario que cada provincia defina los 3 Capítulos reservados: Control, Sanción y Acción de datos personales (materia procesal).

La Dirección Nacional de Protección de Datos Personales (D.N.P.D.P), desde su concepción nació con la idea de la "Red Argentina de Protección de Datos Personales" (RAPDP), proponiendo un sistema de estructuras administrativas provinciales ideado para asegurar la protección de los datos personales en todo el

[12] Art. 5 y 31 de la Constitución Nacional Argentina.

territorio Nacional. Cada estructura se desempeñará como nodo de Red independiente y serán creadas según el criterio de cada provincia, trabajando en conjunto con la Dirección Nacional de Protección de Datos Personales.[13]

Queda claro cuál es la idea a seguir: cada Provincia debería crear su estructura de control y sanción, estableciendo una autoridad de control y creando su Registro Provincial de Datos Personales, trabajando siempre en coordinación con la D.N.P.D.P.

Volviendo a la Figura Nº 2, existe a la fecha, una sola Provincia que ha adherido al régimen nacional, designando su autoridad de control y creando su registro provincial, que es Neuquén.

Mendoza y la Ciudad Autónoma de Buenos Aires, que no han adherido al régimen, han dictado sus propias normativas en materia de datos personales (regulando la parte general), caminando por una peligrosa cornisa, ya que si bien está dentro de las facultades de las Provincias, dichas regulaciones, deben estar siempre en coherencia legislativa con la Ley Nacional. Es decir, la Ley Nº 25.326, debería ser un piso normativo, sobre el que se podría regular de manera más estricta por algún Estado Provincial, pero nunca exigiendo o regulando menos, porque daría lugar a conflictos jurídicos por la doble regulación en discordancia. De allí, el fundamento de nuestra posición.

Pasando en limpio, de las 24 jurisdicciones de nuestro país, sólo 4 (16,6%) han designado su autoridad de control y sanción en materia de datos personales (Misiones, Mendoza, Neuquén y la Ciudad Autónoma de Buenos Aires). De estos 4, Neuquén y CABA ya tienen su registro de bases local; Mendoza creó su REPID (Registro de Empresas Privadas de Información de Deudores) con una clara inclinación hacia la regulación de datos en materia financiera; por último, Misiones aún no tiene creado su Registro, pero es una de las obligaciones pendientes de su órgano de control designado.

¿Deben los Estados Provinciales regular un procedimiento especial para la procedencia de la acción de habeas data?

Si, deben regular porque la materia es procesal y por lo tanto competencia específica de los Estados Provinciales, o bien deben adherirse al régimen de la Ley Nº 25.326, aceptando las reglas procesales que incluye el mismo.

En la Figura Nº 2, se puede observar que de las 24 jurisdicciones de nuestro país, sólo 6 (25%) han regulado de alguna manera este procedimiento (ya sea de manera independiente, como Chubut, o como parte de una regulación integral, como la de Neuquén).

De todas maneras, e independientemente de esta realidad objetiva legislativa, en todas las provincias se han ventilado casos de habeas data, tanto en los juzgados provinciales como federales, generándose una proficua jurisprudencia.

[13] Sitios Oficial de la Dirección Nacional de Protección de Datos Personales; http://www.jus.gov.ar/datos -personales/red-argentina-.aspx

¿Es competente la justicia federal o la local en los casos de habeas data?

En algunos casos la justicia federal, en otros la provincial. La Ley de Protección de Datos Personales 25.326 establece en su artículo 36[14] que, a elección del actor, será **competente** para entender en esta acción el juez: a) del domicilio del actor; b) del domicilio del demandado; c) del lugar en el que el hecho o acto se exteriorice, d) del lugar donde el hecho pudiera tener efecto. Procederá la competencia federal cuando se interponga en contra de archivos de datos públicos de organismos nacionales, o cuando los archivos de datos se encuentren interconectados en redes: interjurisdiccionales, nacionales o internacionales.

Con respecto a la competencia material, el criterio mayoritariamente seguido es aquél por el cual se sostiene que, cuando la situación a tutelar por el habeas data se relaciona con el ejercicio de la función administrativa y los registros o bases de datos pertenecen a la autoridad pública, el fuero competente debe ser el contencioso administrativo (Cfr. C.Cont. Administ. Córdoba, Sala 1, marzo 23/995 in re "García de Llanos, Isabel c/ Caja de Jubilaciones, Pensiones y Retiros de Córdoba").”[15]

En relación a la competencia territorial, creemos que la segunda parte del art. 36 es la que plantea el problema del momento, y que debe ser morigerado por la legislación provincial procesal o interpretado por los jueces, ya que es raro encontrar en la actualidad una base de datos que no esté conectada a Internet. Es importante y coincidente lo que la Corte ha manifestado en varias oportunidades al decir: “Las disposiciones que consagran la jurisdicción federal, que por su naturaleza es limitada y de excepción, se deben interpretar restrictivamente, descartando su aplicación analógica a situaciones que no sean expresamente contempladas en cada caso (confr. Corte Suprema de Justicia de la Nación”[16] Y cuando resuelve que, "dado que las acciones de amparo y habeas data iniciadas contra una empresa de televisión por cable con el fin de conocer los datos personales y antecedentes que dicha entidad tiene del actor, no pone en tela de juicio ninguna materia relativa a cuestiones regidas por la ley 19.798 de telecomunicaciones, ni comprometen la responsabilidad del Estado, no resulta competente para entender en las mismas la justicia federal.”

Sin embargo no podemos dejar de mencionar ciertas dificultades para los tribunales locales que se presentan por lo menos en dos frentes: El primero es el probatorio, ya que no siempre la justicia provincial se encuentra en condiciones de disponer de especialistas certificados en peritaje forense. Esto es subsanable con capacitación de profesionales y adquisición de las herramientas específicas, acciones que deberían profundizarse a la brevedad, antes que el volumen de causas de este tipo genere un nuevo cuello de botella en la administración de justicia.

[14] Si bien el artículo mencionado es parte del Capítulo VII (que es de regulación provincial), es una pauta de referencia para los magistrados.

[15] http://www.portaldeabogados.com.ar/derechoinformatico/gozaini.htm#3. Competencia. EL PROCESO DE HABEAS DATA EN LA NUEVA LEY DE PROTECCION DE DATOS PERSONALES - 1ª parte - Osvaldo Alfredo Gozaini - Para Portal de Abogados

[16] Fallos: 283:429 y 301:511

El segundo problema, mucho más difícil, es el lugar de alojamiento de las bases de datos, las cuales pueden encontrarse tanto en el país como en el exterior, acrecentado ahora a partir de la difusión del "cloud computing"[17].

Recientemente el Tribunal Colegiado Nº 2 de Rosario determinó que las causas contra Facebook o Google deben tramitar ante la Justicia Federal, "si la información que se pretende suprimir fue proporcionada por Internet, que constituye una red interconectada, es claro que deben intervenir en la controversia los jueces federales con competencia civil y comercial" [18].

Si se impusiera la necesidad de litigar en el fuero federal para todo caso de habeas data, por el solo hecho que la computadora "esté conectada a Internet" se produciría un efecto gravoso de acceso a la justicia para los ciudadanos del interior y un exceso de atracción jurisdicional injustificada para los tribunales federales.

Recomendaciones para las Provincias:

1) Que dicten leyes de adhesión a la ley nº 25.326 de datos personales con los siguientes recaudos:

a. No introducir definiciones técnicas ya que estas están en la ley nacional o son propias de la ciencia, máxime en materia de TICs.

b. Tener presente que la ley 25.326 es de orden público en los artículos 1 a 28 y 32 (sanciones penales).

c. Las Provincias deben adherir por lo indicado en el art. 44 a las normas "que fueren de exclusiva e jurisdicción nacional". Ésta expresión es ambigua porque hoy casi todas las computadoras y bancos de datos se encuentran interconectadas a redes de alcance interjurisdiccional e internacional, por lo cual deben establecerse directivas de competencia más precisas, en concordancia a la jurisprudencia.

3) Tienen que reglamentar el procedimiento que se aplicará para el amparo por habeas data, ya que éste no es siempre procedimiento sumarísimo en las distintas jurisdicciones.

4) Deben establecer organismos de control y sanción independientes del Poder Ejecutivo.

5) Deben hacer convenio con la DNPDP.

6) Definir un procedimiento administrativo para el requerimiento a la misma Provincia (por datos públicos provinciales y a las bases de datos sometidas a su jurisdicción).

7) Considerar dentro de la regulación a las cámaras de videos y otros dispositivos callejeros o no pero que pudieran contener datos personales (máquinas de estacionamientos, peajes, colectivos, etc.).

8) Hasta tanto se reglamente la ley, se habilite que las oficinas de consumidores provinciales, asistan a los ciudadanos sobre cuestiones vinculadas a los informes crediticios y financieros.

[17] Según el IEEE Computer Society, es un paradigma en el que la información se almacena de manera permanente en servidores en Internet y se envía a cachés temporales de cliente, lo que incluye equipos de escritorio, centros de ocio, portátiles, etc.

[18] Eljurista.net. Fallo 184/2010. http://bit.ly/bphVIn

9) Admitir el amparo colectivo en tema de protección de datos personales, ya que por la naturaleza de estos casos puede haber muchos afectados en (por ejemplo) el tráfico ilegal de bases de datos.

Conclusión

Creemos que procurándonos una buena legislación, el debido control y responsabilidad social empresaria y corporativa lograremos un círculo virtuoso para la protección de los datos personales, cada vez más abundantes y vulnerables en la Sociedad de la Información.