Revista de Derecho
Comunicaciones y
Nuevas Tecnologías

El sistema legal uruguayo de protección de datos personales

Ana Brian Nougrères

Contenido

"Rest a political system on an unstable undation, and it will crumble under pressure and fall away like sand. But build that system on solid stones, and it will hold up and withstand the tests of time"
Sandra Day´Connor (2003)

EL SISTEMA LEGAL URUGUAYO DE PROTECCIÓN DE DATOS PERSONALES

*Ana Brian Nougrères**

RESUMEN

El presente comienza analizando distintos tipos de sistemas y modelos normativos que amparan el derecho fundamental a la protección de datos. Analiza los modelos que presentan la Unión Europea, los Estados Unidos de Norteamérica, Canadá, para luego irse circunscribiendo a Iberoamérica y América Latina. A continuación describe integración y cometidos de la Red Iberoamericana de Protección de Datos, enumera los documentos aprobados por esta para comentar específicamente uno de ellos. Para finalizar, detalla la situación normativa en la materia en la República Oriental del Uruguay y concluye describiendo el sistema uruguayo en protección de datos personales.

ABSTRACT

The following begins analyzing different regimes for data protection, describes the regulation on data protection and habeas data in the European Union, the United States of America, Canada, Iberoamerica and Latin America. It continues explaining the activities of the Red Iberoamericana de Protección de Datos (Iberoamerican data protection network), which was established as a result of an initiative put forward by the Agencia Española de Protección de Datos (Spanish data protection agency), its constitution, purpose, tasks, and the series of documents approved, in particular the set of norms recently approved (2007) on general principles on data protection. On the last part, the document describes the Uruguayan regime on data protection.

Key Words: Protección de datos personales, Iberoamérica, América Latina, Red Iberoamericana de Protección de Datos, Uruguay. Data protection, privacy, Iberoamerica, Latin America, Iberoamerican data protection network.

* Doctor en Derecho y Ciencias Sociales por la Universidad de la República Oriental del Uruguay. Asesor letrado en el Parlamento uruguayo. Cátedra de Informática Jurídica, Facultad de Derecho, Universidad de la República. Integra la Red Iberoamericana de Protección de Datos Personales desde su creación. Se ha desempeñado como Asesor en materias de informática y derecho del Directorio del Colegio de Abogados del Uruguay, del que ha sido miembro, y ha integrado su Comisión de Informática Jurídica y Derecho Informático. Integra el Instituto de Derecho Informático (Facultad de Derecho) y el Capítulo Uruguay de FIADI. Ha sido ponente y conferencista, ha dictado cursos y ha trabajado y participado en eventos académicos y profesionales, con técnicos de distintas universidades e instituciones, en temas vinculados con informática y derecho, así como con protección de datos, en su país (Intendencias de Montevideo y Rivera, IMPO, Cámara Uruguaya de Comercio y Servicios, Facultad de Derecho, Grupo de Investigación Núcleo Derecho Civil) y en el exterior (Buenos Aires, París, Milán, La Habana, Montevideo, Florencia, Lima, Roma, México, Madrid, Guatemala, Córdoba, Stanford, Colombia, Bolivia, Berlín, Chile, Tokio). Dirección electrónica: abrian@netgate.com.uy.

INTRODUCCIÓN

La doctrina que ampara la protección de los datos personales es consecuencia de una preocupación creciente por el avance de los medios tecnológicos de información y comunicaciones, que proveen de la potencialidad de manipular la información atentando sobre la libertad, la vida y la dignidad de las personas. La tecnología ha evolucionado a pasos tan agigantados que ha llevado a conformar un nuevo diseño del mundo, de las formas de comunicación, de socialización, de educación, de trabajo, de encarar los problemas de salud, la cultura y el desarrollo social, y han ido transformando la información en un factor clave, que posee un valor de mercado, al punto que nosotros mismos nos hemos transformado en objeto de información en todos y cada uno de nuestros actos.

En este contexto, la tutela del derecho a la intimidad de las personas se ha constituido en una de las garantías más importantes para el ciudadano, que en el desarrollo de la sociedad de la información adquiere una relevancia aún mayor ya que las nuevas herramientas hacen posible "no sólo planear las bases de un desarrollo más integral de la persona y alcanzar algunos sueños democráticos, como lo es la posibilidad de que cada ciudadano se interese por los asuntos públicos y pueda intervenir directamente en las decisiones que puedan afectar sus derechos, sino que también engendran graves peligros, ya que facilitan el manejo, organización y comparación de una gran cantidad de datos sobre los ciudadanos, los cuales pueden así ser utilizados para controlarle y limitarle sus ámbitos de libertad"[1].

La necesidad de regular el principio de la autodeterminación informativa surge, en esta coyuntura, concediendo a cada individuo el poder de gobierno sobre la circulación de la información sobre los datos de que es titular. Ahora bien, más allá de lo que puede interpretarse como un enfoque privatista e individual de este derecho a decidir sobre los propios datos, ha surgido una nueva concepción de este derecho no "como una facultad del individuo aislado, sino como un derecho de coexistencia ... la esfera de la personalidad no puede contemplarse únicamente desde el punto de vista del individuo, sino desde una perspectiva relacional desde la que se considera que la violación de la personalidad humana comporta una situación de peligro para la solidaridad y la convivencia entre los hombres"[2].

El derecho a la protección de datos personales nace como una garantía para el individuo en el ejercicio de sus derechos fundamentales, una garantía de que él es un elemento clave en lo que refiere al control en la comunicación o utilización de sus datos de carácter personal.

Los datos personales han asumido un papel importante en la sociedad de mercado, y esto ha traído riesgos consiguientes a las personas, en tanto las posibilidades que otorgan las tecnologías de inspeccionar la vida íntima de cada persona son cada vez mayores. Las costumbres, las inclinaciones, las dependencias, los vicios, corren el riesgo de salir de los ámbitos reservados de cada persona y pasar a ser observados y registrados por el estado o por los particulares, de una forma sencilla, rápida, que opera sin que sea percibida por el titular de los datos. El control, la vigilancia, la intromisión, con la ayuda de las tecnologías, operan inadvertidamente, muy rápidamente y de una manera muy amplia, lo que hace a los ciudadanos un objeto absolutamente cristalino y transparente. Esa recolección y/o recuperación de nuestros datos por terceros, que incluso pueden llegar a entrecruzar la informa-

1 CHIRINO SANCHEZ, Alfredo, "Autodeterminación informativa y Estado de Derecho en la sociedad tecnológica. Una contribución al estudio de los retos y problemas existentes para alcanzar la protección del ciudadano rente al tratamiento electrónico de sus datos personales", trabajo inédito.

2 PÉREZ LUÑO, Antonio Enrique, "Derechos humanos, estado de derecho y constitución", 3ª. Ed., Editorial Tecnos, Madrid, p. 326.

ción contenida en diferentes bases de datos, nos lleva a la necesidad de una regulación de la forma cómo ha de ser manejada la información.

Proteger los datos personales de los individuos es proteger no sólo su privacidad, sino también su dignidad, su igualdad y su libertad. Encarar el análisis de un sistema integral de protección de datos nos hace trabajar hacia una sociedad más igualitaria, en que la intimidad no es un privilegio de unos pocos, y en que el acceso a los medios de información está al alcance de todos.

El derecho de acceso a la información y el derecho a la protección de datos personales —ambos derechos de nueva generación— se presentan como formas de tutela de los ciudadanos a diferentes niveles por lo que, si bien no puede decirse que exista a priori una verdadera colisión, pugna o conflicto, es importante que las cuestiones que les atañen sean resueltas de manera armónica. "El tema es de especial relevancia, ya que muchas veces parecería que ambos derechos entran en conflicto, mientras que en otras ocasiones se complementan en contextos donde los órganos del Estado o alguna entidad pública deben rendir cuentas a las personas"[3]. "Los derechos pueden contraponerse cuando se hace una solicitud de acceso a información personal que se encuentre en poder de un organismo gubernamental. Ambos derechos también pueden utilizarse para permitir a los individuos acceder a sus propios datos y así promover la rendición de cuentas gubernamental"[4]. A su vez, cuando se trata de información íntima contenida en bancos de datos, el derecho de cada individuo de controlar su información personal en poder de terceros (caso de información financiera o clínica), debe ser un derecho consistente, así como lo deben ser las reglas para la recolección y el manejo de los datos.

La regulación de ambos temas es deseable que se realice de manera complementaria, que no exista desequilibrio entre el derecho de acceso y el derecho a la protección de datos personales, que se trate de una regulación complementaria, de manera que los puntos de tensión se vean minimizados y que el ciudadano pueda sentir que tiene garantizado el conocimiento y la disposición de la información de la que es titular que se encuentra en bases de datos ajenas.

Mientras que el acopio y la manipulación de la información pueden transformarse en factores de dominación política, social y económica, cuyos límites o salvaguardas es preciso que sean marcados normativamente a efectos de prevenir conductas de discriminación, que atenten contra el derecho a la libertad, a la privacidad, a la dignidad humana, la protección de datos personales es una herramienta necesaria para defender a la sociedad de una excesiva libertad en la colecta y administración de los datos personales, que puede transformarse en flagrante violación a los derechos humanos de los ciudadanos.

El derecho a la protección de los datos personales se presenta como un elemento esencial para el libre desarrollo de la personalidad de las sociedades democráticas[5], que propende a un flujo adecuado de información[6]. La protección de datos garantiza la capacidad de la persona de comunicar y participar y, por lo tanto, es un elemento determinante tanto para la existencia como para la función de una sociedad democrática[7].

3 Declaración de México (2005). "*El acceso a la información pública y la protección de los datos personales*", Anexo a la Declaración Final del IV Encuentro Iberoamericano de Protección de Datos Personales, México.

4 BANISAR, David, "*Two sides of the same coin: conflicts and complements between privacy and freedom of information laws*" Manuscrito, 2005, pp.1 y 2.

5 RODOTA, Stefano (2004), "*Tecnología y derechos fundamentales*", en Revista Datos Personales N° 8, Comunidad de Madrid, España, versión digital compulsable en www.datospersonales.org

6 No en vano se ha dicho que existe una relación de proporcionalidad directa entre el grado de democracia de un país y el número de informaciones que circulan en ella.

7 SIMITIS, Spiros (2005), "*Los fundamentos políticos y sociales de la protección de datos*", en Revista Datos

Los principios en materia de protección de datos[8] establecen una fuente importante para la regulación de la protección de datos en el mundo. En ellos habrán de fundarse las propuestas normativas sobre protección de datos, así como las buenas prácticas.

Los sistemas jurídicos para la protección de los datos personales están conformados por marcos analíticos para la evaluación de los flujos de información, comprensivos de reglas para el tratamiento de los datos personales, que incluyen derechos y acciones del titular de los datos y consagran específicamente la figura del responsable por la colecta y el tratamiento de la información. El tratamiento de estos datos habrá de estar legitimado por el consentimiento de su titular o por una ley dictada en razones de interés general. Las reglas que delinean tal actividad han de incluir la definición de cuáles datos son objeto de protección, si algunos datos ameritan protección diferencial con respecto a otros, así como la finalidad del tratamiento y la limitación en el uso de los datos. Así, los datos pertenecientes a archivos secretos del estado, a registros criminales, los datos sensibles, los datos anónimos, cada uno de ellos ha de tener un tratamiento diferente de otros. A su vez, conforme cuál sea el modelo a seguir, el sistema podrá requerir el establecimiento de una autoridad de control independiente a efectos de conformar el grado de protección que se pretende.

Los modelos de protección de datos son muy variados, acordes con coyunturas de tiempos y lugares. Según el grado de protección que se logra en cada coyuntura espacio-temporal, según cuál sea el esquema legal al efecto y de qué forma juega su rol el uso de la fuerza para hacer valer los derechos de los ciudadanos —en tanto titulares de sus datos—, hay ciertas pautas comunes que los caracterizan como modelos con preeminencia legal, sectoriales, de auto-regulación, de co-regulación.

El modelo europeo tiene por fundamento lo dispuesto en la Directiva 1995/46/CE, relativa a la protección de datos personales y la libre circulación de estos, la Directiva 1997/66/CE, relativa al tratamiento de los datos personales la protección a la intimidad en el sector de las telecomunicaciones y la Directiva 2002/58/CE, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, también conocida como "Directiva sobre la privacidad y las comunicaciones electrónicas", que ha venido a complementar y reactualizar las previsiones contenidas en la normativa comunitaria [9].

Priorizando la armonización de alto nivel en materia de protección de datos en los estados comunitarios y en el marco internacional, subordina la libre circulación de los datos personales a la presencia de un nivel mínimo de protección equivalente. En tal sentido la Directiva 1995/46/CE se destaca por su relevancia en la regulación de este derecho fundamental al proveer acerca del régimen para que operen las transferencias internacionales de datos. Pueden resumirse sus novedades en: ampliación de su ámbito, regu-

Personales N° 17, Comunidad de Madrid, España, versión digital compulsable en www.datospersonales.org.

8 Se trata de: principio de la adecuada recolección y procesamiento de los datos; principio de precisión; principio de la finalidad, finalidad para la especificación y para la limitación; principio de proporcionalidad; principio de transparencia; principio de la participación individual, garantía del derecho de acceso al titular de los datos; principio de no discriminación; principios para la seguridad de los datos; principio de responsabilidad; principio de la independencia de la supervisión y de la sanción legal; principios para un adecuado nivel de protección en caso de flujo transfronterizo de datos personales. Enumeración de principios contenida en la Conclusión 17 de la Declaración Final emitida en ocasión de la Reunión Anual de Comisionados de Protección de Datos 2005 (la traducción nos pertenece), Montreux, Suiza, septiembre de 2005.

9 PIÑAR MAÑAS, José Luis (2003). "*El derecho fundamental a la protección de datos personales*". En: Protección de Datos de Carácter Personal en Iberoamérica. Tirant lo Blanch. Valencia, España, 2005, p. 21.

lación del encargado del tratamiento, desarrollo de los principios de calidad de los datos, el "interés legítimo" como legitimador del tratamiento, cláusula sobre libertad de expresión, reconocimiento del derecho de oposición, reconocimiento de los derechos relacionados con las decisiones individuales automatizadas, desarrollo de sistemas de autorregulación sectorial, régimen sistemático de las transferencias internacionales de datos, reforzamiento de las funciones de las autoridades de protección de datos y creación del Grupo del artículo 29[10].

En tal sentido, se puede apreciar la existencia de leyes que gobiernan la colecta, el uso y la diseminación de la información personal en los sectores público y privado y la existencia de una autoridad que tiene a su cargo la puesta en práctica efectiva del sistema de control. La autoridad de control viene a cumplir la función preventiva, educativa, y también la función de investigar posibles incumplimientos legales e incluso punir los incumplimientos. El poder punitivo del órgano de control varía según los países, y nos permite evaluar un mayor o menor grado de cumplimiento de las normas respectivas.

El modelo de los Estados Unidos de Norteamérica [11] nos muestra la protección de datos personales en leyes que refieren a ramos específicos de actividad. Así por ejemplo existen leyes que delimitan conductas y especifican niveles de protección de los datos para el registro de los alquileres de películas en los videoclubes, o de las transacciones financieras, o los registros de crédito, o los registros de datos médicos. Este modelo de protección, por carecer de una autoridad central, puede generar situaciones de conflicto ante la existencia de normas regulatorias que se superpongan o aspectos de la vida de los ciudadanos que no son especialmente protegidos por el sistema.

En los Estados Unidos de Norteamérica[12] este sistema convive con el sistema de auto-regulación, que nos muestra cómo las distintas empresas, o las industrias, según sus ramas de actividad, generan prácticas de conducta que proveen de normativa de protección de datos a las personas, aunque son esquemas de funcionamiento que no siempre se muestran eficaces en caso de incumplimiento.

El modelo canadiense, por su parte, nos muestra una variante del modelo regulatorio, en que los grupos de interés particulares, representando el comercio y las industrias, coadyuvan con el estado y los usuarios para modelar un sistema adecuado de protección de datos y conformar una agencia de contralor de los datos personales y de acceso a la información que cumpla con su propósito en forma óptima.

Cada modelo de protección de datos conforma un sistema para dicha protección, con caracteres propios y diferenciados.

10 PUENTE ESCOBAR, Agustín (2003). "*Breve descripción de la evolución evolución histórica y del marco normativo internacional del derecho fundamental a la protección de datos de carácter personal*". En: Protección de Datos de Carácter Personal en Iberoamérica. Tirant lo Blanch. Valencia, España, 2005, pp. 59 y 60.

11 SWIRE, Peter P. y BERMANN, Sol (2007). "*Information Privacy. Official Reference for the Certified.Information Privacy Professional (CIPP)*". International Association of Privacy Professionals (IAPP). York, Maine, Estados Unidos de Norteamérica, p. 5.

12 SWIRE, Peter P. y BERMANN, Sol (2007). "*Information Privacy. Official Reference for the Certified Information Privacy Professional (CIPP)*". International Association of Privacy Professionals (IAPP). York, Maine, Estados Unidos de Norteamérica, p. 5.

LA SITUACIÓN EN IBEROAMÉRICA Y AMÉRICA LATINA

En algunas constituciones iberoamericanas la acción de habeas data está consagrada explícitamente[13, 14, 15], en otras tácitamente junto con elementos propios de la protección de datos personales[16, 17], y en el resto —con una concepción de carácter ius naturalista— se encara este derecho dentro de los principios generales del derecho[18].

En la península ibérica, tanto España como Portugal poseen desarrollos normativos que cumplen con los requisitos del modelo europeo.

Por su parte, los países latinoamericanos poseen ordenamientos normativos que en términos generales son comprensivos de disposiciones sectoriales que regulan la protección de datos para determinados tipos de actividad[19, 20], definen los datos sensibles[21], regulan el requerimiento del consentimiento expreso[22], y el derecho de oposición del interesado[23], así como también, en algunos casos, proveen sobre el habeas data[24] o sobre el derecho de acceso[25].

13 Véase, en tal sentido, la Constitución de la República Federativa de Brasil (1988), que consagra el habeas data en el artículo 5º numeral LXXI de su capítulo sobre Derechos y Garantías Fundamentales.

14 Del mismo modo, la Constitución paraguaya (1992) que consagra específicamente y con carácter amplio el habeas data en su artículo 135 y la acción de amparo en su artículo 136.

15 También en la República de Ecuador, el artículo 30 de la Constitución establece "Toda persona tiene derecho a acceder a los documentos, bancos de datos e informes que sobre sí mismos o sobre sus bienes consten en entidades públicas o privadas, así como a conocer el uso que se haga de ellos y su finalidad".

16 Es el caso de la Constitución portuguesa (1976) que, en su artículo 35, luego de consagrar en su numeral 1 la acción de amparo, establece en su numeral 2 que la informática no se podrá utilizar "para el tratamiento de datos referentes a convicciones políticas, fe religiosa o vida privada, salvo cuando se trate de la elaboración de datos no identificables para fines estadísticos".

17 También la Constitución colombiana que, en su artículo 15, dice: "Todas las personas tienen derecho a su intimidad personal y familiar. De igual modo, tienen derecho a conocer, actualizar y rectificar las información que se hayan recogido sobre ellas en bases de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución..."

18 Es el caso de la Constitución uruguaya (1967), que analizaremos más adelante.

19 Tal es el caso de Chile para datos públicos, en tanto la Ley Orgánica de Bases de la Administración del Estado (DFL 1, de 2001, del Ministerio Secretaría General de la Presidencia) establece que el Servicio de Registro Civil e Identificación llevará el registro de las bases de datos personales a cargo de los organismos públicos, en el cual se inscribirán todas las bases de datos personales que, de acuerdo con la ley respectiva lleven las autoridades, órganos del estado y organismos descritos y regulados por la Constitución Política de la República y los comprendidos en el inciso 2 del artículo 1° de la Ley N° 18.575 que organiza las bases generales de la administración del estado.

20 También Perú, desde el año 2001, en que comenzó a regir la Ley Nº 27488, se reguló la actividad de las centrales privadas de información sobre riesgos y la protección al titular de la información.

21 En tal sentido, en Paraguay, la Ley N° 1682, en la redacción dada por la Ley N° 1969, artículo 4° establece que aquellas personas que sean individualizadas o individualizables explícitamente, son protegidas por este artículo que prohíbe la publicación o difusión de sus datos sensibles, considerados como tales, los raciales, étnicos, políticos, salud, sexuales, filosóficos, religiosos, morales, y en general que puedan fomentar prejuicios, discriminaciones o afecten la dignidad, la privacidad, intimidad doméstica la imagen privada de personas o familias".

22 En Argentina, la Ley N° 25326, en su artículo 5°, refiere al consentimiento expreso, libre, informado y deberá constar por escrito o por un medio distinto a la forma escrita cuyos requisitos los establecerá la Dirección Nacional de Protección de Datos Personales (artículo 5 del decreto 1558/2001).

23 La Ley N° 17838, artículo 17 numeral 2, establece ken el caso uruguayo, la posibilidad del interesado de solicitar al responsable de la base de datos su rectificación, eliminación o supresión.

24 En Brasil, el habeas data tiene consagración en la Constitución Federal de 1988, artículo 5° inc. LXXII, que preceptúa "Se concederá el habeas data: a) para asegurar el conocimiento de informaciones relativas a la persona del solicitante, constancias de registros o bancos de datos de entidades gubernamentales o de carácter público; y b) para la rectificación de datos, cuando no se prefiera hacerlo a través de un procedimiento reservado, judicial o administrativo. A su vez, por Ley N° 9507, se regula en Brasil el derecho de acceso a informaciones de carácter personal y se disciplina el proceso de habeas data.

25 Es el caso de México, que se destaca por poseer una Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, fechada 11 de junio de 2002,

Los sistemas de protección de datos de los países latinoamericanos tienen su fundamento en disposiciones normativas, en algunos casos constitucionales, que se ven complementadas en desarrollos jurisprudenciales, que ante disposiciones escasas han llenado vacíos e incluso han desarrollado principios esenciales en torno al derecho a la protección de datos personales[26]. En términos generales no llegan a un grado de regulación exhaustiva como es el caso del modelo europeo. Basan su sistema en normativa sectorial, que es complementada con disposiciones marco que acogen la protección de datos personales y el derecho de acceso con un mayor o menor grado de explicitación, según los distintos ordenamientos.

La República Argentina es el único país latinoamericano que actualmente posee un modelo de protección de datos que sigue fielmente la línea europea.

En tal sentido, la Constitución de la Nación Argentina (1994), en su artículo 43, regula la acción de amparo para toda aquella persona que procure "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 aquellos...", consagrando de esta forma lo que la doctrina denomina libertad informática.

A su vez, la Ley 25.326 (2000) de Protección de Datos Personales, sigue el modelo de la Directiva europea No. 95/46/EC, conformándose así, junto con su decreto reglamentario (n° 1558/2001), un sistema que contiene disposiciones que regulan los principios generales en la materia, así como los derechos de los titulares de los derechos, las obligaciones de los usuarios, las funciones de la autoridad de control —la Dirección Nacional de Protección de Datos que depende del Ministerio de Justicia— y el procedimiento para la tutela de los datos personales.

En este esquema de funcionamiento, la Unión Europea ha conferido a Argentina la categoría de país con un nivel adecuado de protección de datos[27], habilitando por consecuencia la transferencia internacional de datos personales entre Argentina y la Unión Europea.

El caso argentino, por poseer un sistema de protección de datos conforme el modelo europeo, se constituye en un caso aislado de los demás países latinoamericanos, y en tal sentido más cercano al modelo que en Iberoamérica dan España y Portugal.

que establece que toda información que poseen los tres poderes federales, legislativo, judicial y ejecutivo, que incluye a las entidades y dependencias de la administración pública federal, así como los órganos constitucionales autónomos y cualquier otro órgano federal, es pública, excepto aquella que es clasificada como reservada o confidencial. Se entiende por información reservada la que compromete la seguridad, las relaciones internacionales, la estabilidad financiera, pone en riesgo de vida a las personas o provoca perjuicio a las actividades de verificación del cumplimiento de las leyes. Por información confidencial referimos a los datos personales de cualquier individuo referentes a su domicilio, teléfono, expediente médico, origen racial o étnico, características físicas, morales o emocionales toda aquella que afecte su intimidad. Crea, a su vez, el Instituto Federal de Acceso a la Información Pública, cuyo cometido es garantizar el cumplimiento de la Ley Federal de Acceso a la Información Pública Gubernamental y promover el derecho de acceso a la información pública y la protección de datos personales.

26 BARTH JIMENEZ, José Francisco (2003) "Marco normativo y jurisprudencial de la protección de datos en Costa Rica". En: *Protección de datos de carácter personal en Iberoamérica*. Ed. Tirant lo Blanch, Valencia, 2005.

27 Dictamen 4/2002, de adecuación de la República Argentina a la Directiva 95/46/CE, emitido por el Grup de Trabajo del artículo 29.

LA RED IBEROAMERICANA DE PROTECCIÓN DE DATOS

INTEGRACIÓN Y COMETIDOS

La Red Iberoamericana de Protección de Datos fue establecida como resultado de una iniciativa de la Agencia Española de Protección de Datos, en ocasión del II Encuentro Iberoamericano de Protección de Datos llevado a cabo en La Antigua, Guatemala, en Junio de 2003[28].

Fue concebida como un foro permanente, abierto a la incorporación de representantes de todos los países iberoamericanos, que constituyen la comunidad iberoamericana de naciones, con el propósito de potenciar las iniciativas de difusión de información e intercambio de experiencias entre las naciones, así como para fortalecer los vínculos mutuos de cooperación recíproca en materia de protección de datos, estableciendo canales permanentes de diálogo y colaboración en materia de protección de datos. Está en su ánimo buscar y sugerir soluciones armonizadas, así como apoyar las iniciativas para difundir y desarrollar la cultura de protección de datos personales en los países latinoamericanos en un contexto democrático.

En esta misma Declaración de La Antigua Guatemala referida, los representantes de Argentina, Brasil, Chile, Colombia, Costa Rica, El Salvador, España, Guatemala, México, Nicaragua, Perú, Portugal y Uruguay manifiestan que "8º - Son conscientes de que el derecho a la protección de datos personales fortalece el Estado de Derecho y ayuda a reforzar la democracia en los Países Iberoamericanos, así como su prestigio y credibilidad en un mundo globalizado. A tal fin, y en el marco legal e institucional de sus respectivos países, realizarán, dentro de sus respectivas competencias, los esfuerzos necesarios para que la protección de datos personales sea impulsada en el seno de la Conferencia Iberoamericana, en la certeza de que así se promoverá la difusión y concienciación de tan importante derecho fundamental".

Poco después, en Noviembre de 2003, durante la XIII Cumbre Iberoamericana de Jefes de Estado y Gobierno llevada a cabo en Santa Cruz de la Sierra, Bolivia, se declaró "somos conscientes de que la protección de datos personales es un derecho fundamental de las personas y destacamos la importancia de las iniciativas regulatorias iberoamericanas para proteger la privacidad de los ciudadanos contenidas en la Declaración de La Antigua, por la que se crea la Red Iberoamericana de Protección de Datos, abierta a todos los países de nuestra Comunidad[29].

En términos similares, en la Declaración Final emitida en la 27ª Conferencia de Comisionados y Protección de Datos llevada a cabo en Montreux, Suiza, en Setiembre de 2005, nuevamente se reconoció la importancia de las actividades de esta Red.

La Red Iberoamericana de Protección de datos está integrada por representantes de 17 de los 22 países de la comunidad iberoamericana. Su número de representantes, así como su rápido crecimiento en tan escaso tiempo, demuestra el interés que sus actividades han despertado en la región.

Una de las tareas más importantes asumidas por la Red es la del fomento del mejoramiento de los instrumentos de regulación de la protección de datos personales, como una forma de asegurar el respeto de este derecho fundamental en los países iberoamericanos en los cuales la legislación al respecto está pendiente de aprobación. De esta manera, se procura la unicidad de los criterios en los distintos regímenes de protección de datos, a efectos de trabajar en pos de un standard de protección. A tales efectos, se

28 Declaración de La Antigua, numeral 7º.

29 Declaración de Santa Cruz de la Sierra, numeral 45.

crea una red de intercambio de datos entre los países iberoamericanos, cuyo fin último es el mejoramiento de las relaciones comerciales y del comercio internacional en esta parte del mundo globalizado.

La Red Iberoamericana de Protección de Datos ha tenido Encuentros anuales, desde su creación en 2003. Estos Encuentros se han constituido en una plataforma para los países miembros de la Red para el intercambio de experiencias y la discusión de las últimas innovaciones en protección de datos personales. Los temas fundamentales tratados en cada Encuentro son publicitados en Declaraciones, que normalmente contienen las posiciones comunes en las diferentes temáticas traídas al análisis por los países miembros.

En el III Encuentro Iberoamericano de Protección de Datos llevado a cabo en Cartagena de Indias, Colombia, en junio de 2004, se decidió incorporar a las actividades de la Red estudios más profundos sobre los temas que conciernen a protección de datos, sin dejar de lado los objetivos de cooperación y asistencia recíproca entre los países en materia de protección de datos personales.

Consecuencia de la conformación de estos grupos de trabajo han sido los documentos que sobre diversa temática ha aprobado la Red. A saber[30]: protección de datos y la perspectiva del sector financiero (Cartagena de Indias, 2004), lucha contra el spam (Cartagena de Indias, 2004), transferencias internacionales de datos: perspectivas europeas e iberoamericanas (Cartagena de Indias, 2004), el sector de las telecomunicaciones e internet ante los ataques de la privacidad (Cartagena de Indias, 2004), el sector comercial y el uso de la información con fines de marketing (Cartagena de Indias, 2004), viabilidad de creación de autoridades de control en el entorno latinoamericano (México, 2005), gobierno electrónico y telecomunicaciones (México, 2005), acceso a la información pública y protección de datos (México, 2005), impulso normativo y armonización (Santa Cruz de la Sierra, 2006), red "on-line" (Santa Cruz de la Sierra, 2006), instrumentos de autorregulación (Santa Cruz de la Sierra, 2006), tratamiento de datos en salud en relación con la historia clínica (Santa Cruz de la Sierra, 2006), directrices para la armonización de la regulación de la protección de datos en la comunidad iberoamericana (Cartagena de Indias, 2007).

De estos, por la importancia de la función armonizadora de las soluciones a los distintos problemas que presenta la necesidad de proteger los datos personales de los ciudadanos iberoamericanos, haremos especial referencia a las Directrices para la Armonización de la Regulación de la Protección de Datos aprobadas en mayo de este año 2007, en Cartagena de Indias, Colombia.

DIRECTRICES PARA LA ARMONIZACIÓN DE LA REGULACIÓN DE LA PROTECCIÓN DE DATOS EN LA COMUNIDAD IBEROAMERICANA

Generalidades

El cometido de las presentes Directrices es coadyuvar en pos de la armonización como fundamento primero en la adopción de instrumentos internacionales, garantizar la compatibilidad del desarrollo del comercio con la protección de datos y constituirse en un marco homogéneo de regulación.

Para la consecución de sus fines, las directrices propenden a la creación de instrumentos supranacionales vinculantes entre los estados, leyes nacionales que contengan la consagración del derecho fundamental a la protección de datos, cláusulas contractuales e instrumentos de autorregulación.

30 Todos estos documentos pueden consultarse en www.agpd.es.

Como consecuencia de la aplicación de las Directrices se producirá la equiparación de la normativa del país que da origen a la transferencia internacional de datos con la normativa del país europeo que recibe la transferencia internacional de datos, procurando de esa forma un beneficio para ambas partes y el fomento del comercio entre los estados, viéndose de esta manera a la cooperación como un medio para lograr un marco homogéneo en la protección de datos personales.

Estas Directrices tienen por finalidad el fortalecimiento de la cooperación científica y técnica, el establecimiento coordinado de nuevas redes de telecomunicaciones, el facilitamiento de la circulación transfronteriza de datos garantizando niveles de protección de los derechos y libertades de las personas. Procuran el tratamiento equivalente y el nivel de protección de derechos y libertades, la coherencia en la regulación normativa y generar un marco homogéneo en protección de datos personales, coadyuvando en definitiva al desarrollo del comercio.

Se pretende conformar una sociedad con cultura en materia de protección de datos personales, consciente de los principios que informan la protección, de sus derechos y de las responsabilidades consiguientes, con un órgano de control fuerte y una acción de habeas data operativa.

Dados estos presupuestos, analizado el caso en la Unión Europea, el grupo de trabajo del artículo 29 de la UE emitió el dictamen n° 4/2002, que dio lugar a la consideración de la República Argentina como un país con un régimen de protección de datos adecuado al de la Unión Europea. A estos efectos el mencionado grupo de trabajo tuvo en cuenta que la legislación del país hermano recogía los principios básicos de protección de datos personales, que existían los mecanismos de control de dichos principios, que se había creado una autoridad independiente de protección de datos, que había regulación normativa de procedimientos adecuados para la protección de los datos personales y para la reparación de los perjuicios provocados por la violación al derecho fundamental a la protección de datos personales.

Análisis de su articulado

Este cuerpo normativo contiene diez directrices que tratan de los principios en materia de protección de datos personales, los derechos, las obligaciones, autoridad de control y acciones.

La Directriz 1 refiere al ámbito de aplicación y establece —como principio— que su aplicación es a todo tratamiento de datos referido a personas identificadas o identificables, con tres excepciones, según se detalla a continuación.

La primera excepción determina que puede excluirse de las directrices el tratamiento manual o no automatizado cuando no vaya a ser incorporado a un fichero estructurado conforme criterios que permitan identificar las personas cuyos datos son sometidos a tratamiento. La segunda excepción nos indica que no serán aplicables a los datos personales que una persona física realice con fines exclusivamente relacionados con su vida privada o familiar. La tercera excepción marca una exclusión a las directrices n° 2, 3, 4, 5, 6.1, 6.2, 6.3, y 8, y requiere que la exclusión se realice mediante ley nacional, cuando pueda suponerse un riesgo para la seguridad nacional, el orden público, la salud pública o la moralidad; en el caso, los tratamientos de datos deben resultar estrictamente necesarios y deben resultar no excesivos en el ámbito de la sociedad democrática.

La Directriz 2 establece los principios de tratamiento leal y lícito, limitación de la finalidad, proporcionalidad, exactitud, conservación.

La Directriz 3 conforma la legitimación para el tratamiento de los datos, que se da con el otorgamiento del consentimiento del titular de los datos. El consentimiento se entiende necesario

—por principio— al efecto de recabar y de tratar los datos.

A este principio cabe el excepcionamiento, siempre que sea consagrado legalmente, que la excepción no perjudique los derechos fundamentales del interesado y que el tratamiento u obtención de datos se realice en el marco de una relación jurídica o por una administración en el ejercicio de sus potestades legalmente atribuidas.

En el caso de datos sensibles que refieran a ideología, afiliación sindical, religión, creencias, el principio es el consentimiento y la única excepción puede darse en el caso en que el titular del dato lo hizo manifiestamente público.

En el caso de los datos sensibles que refieren a salud, origen racial o vida sexual también el principio es el consentimiento. La excepción en este caso puede darse en dos casos, el primero: si el interesado los hizo manifiestamente públicos, el segundo: por ley siempre que no se obstaculice el adecuado tratamiento médico del interesado, ni la atención de una urgencia vital.

La Directriz 4 refiere a la obligación de transparencia en la recogida de datos acerca de quién es el responsable por el tratamiento de los datos, de los fines para los que los datos serán tratados, del modo en que se podrán hacer efectivos los derechos a la protección de los datos, y de cualquier otra información necesaria para la garantía del tratamiento lícito de los datos. Asimismo, en el caso de que los datos no fueran obtenidos directamente de su titular, deberá informársele acerca de los extremos indicados anteriormente en un plazo prudencial, siempre antes de que los datos sean comunicados a un tercero.

La Directriz 5, en lo que hace a la forma de ejercer el derecho de acceso, establece que los procedimientos deben ser claros, expeditos, gratuitos y que no deben provocar gastos excesivos al interesado.

En cuanto al objeto del derecho de acceso, establece que es la existencia o inexistencia del tratamiento de los datos que le conciernen, la información acerca de los fines de dichos tratamientos, las categorías de datos a que se refieran, los destinatarios o las categorías de destinatarios a los que se harán llegar los datos, así como los datos objeto de tratamiento y toda la información disponible sobre el origen de los datos.

También esta misma Directriz 5 establece los presupuestos de los derechos de rectificación y cancelación, que son: que los datos aparezcan incompletos, inexactos, inadecuados o excesivos. En estos casos, también cabe exigir que se notifique a los terceros a quienes se hayan comunicado los datos de toda rectificación o cancelación efectuada.

La Directriz 6 "Otros derechos de los interesados" establece que estos interesados no han de "verse sometidos a decisiones con efectos jurídicos sobre ellas o que les afecte de manera significativa, que se basen únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, como su rendimiento laboral, crédito, fiabilidad o conducta. No obstante, será posible la adopción de dichas decisiones cuando se verifiquen en el marco de una relación jurídica libremente aceptada por el interesado, en que se concede a la misma la posibilidad de efectuar alegaciones acerca del resultado de la valoración".

Establece esta Directriz, asimismo, que los interesados tendrán derecho a "oponerse al tratamiento de sus datos, en supuestos no excluidos en virtud de la Ley, como consecuencia de la concurrencia de una razón excepcional y legítima derivada de su concreta situación personal".

Asimismo, tendrán derecho a oponerse, previa petición y sin gastos, al tratamiento de los datos de carácter personal que les conciernan respecto de los cuales el responsable vaya a llevar a cabo

un tratamiento para actividades vinculadas con la publicidad y la prospección comercial.

También podrán los interesados recabar el auxilio de los tribunales y de las autoridades de control en caso de considerar que el tratamiento de sus datos se está llevando a cabo con conculcación de lo dispuesto en las directrices.

Además, tienen derecho a ser indemnizados por cualquier daño o lesión que hubieran sufrido en sus bienes o derechos como consecuencia del tratamiento de datos llevado a cabo con conculcación de lo dispuesto en estas directrices.

La Directriz 7 refiere a la seguridad y confidencialidad en el tratamiento de los datos, habla de las medidas técnicas y organizativas necesarias para proteger los datos contra su adulteración, pérdida, destrucción accidental, acceso no autorizado, o uso fraudulento, además de hacer referencia al secreto profesional.

La Directriz 8, por su parte, establece limitaciones a la transferencia internacional de datos, marcando como regla general que sólo podrán efectuarse transferencias internacionales de datos al territorio de estados cuya legislación recoja lo dispuesto en las presentes directrices.

Al principio general sobre transferencia internacional de datos se marcan dos excepciones. La primera, por ley, atendiendo a las circunstancias que concurran en cada supuesto, teniéndose en cuenta los derechos e intereses del afectado y, en particular, si el mismo ha prestado su consentimiento a la transferencia en cuestión. La segunda, para el caso de que se obtenga la autorización de la autoridad de control respectiva, en cuyo caso será necesaria la aportación por parte del exportador de garantías suficientes para asegurar que el importador cumplirá en todo caso lo dispuesto en estas directrices.

La Directriz 9 refiere a autoridades de control, cuyo cometido es velar por el cumplimiento de los principios en la materia y atender que los ciudadanos puedan efectuar sus reclamaciones. A tal efecto han de poseer poderes de investigación, inspección y averiguación, así como capacidad para imponer sanciones, competencia para instar a los tribunales a la imposición de medidas ante la vulneración de los principios y posibilidad de adoptar las medidas necesarias para evitar la persistencia en el incumplimiento de lo dispuesto en las directrices.

Esta misma Directriz estructura los requisitos que ha de cumplimentar toda autoridad de control, que debe poseer independencia en su actuar e imparcialidad. No debe estar sometida en el ejercicio de sus funciones al mandato de ninguna autoridad pública, su independencia debe estar garantizada. También, las personas a cuyo cargo se encuentre la dirección de dichas autoridades de control deberán ser inamovibles.

Con independencia de ello, podrán implementarse sus funciones a cargo de una o varias autoridades, puede tratarse de autoridades con personalidad propia o que estén integradas en la administración pública, puede tener por función la relativa a la protección de datos personales, o puede tener otras competencias legalmente atribuidas.

La autoridad de control tendrá por competencia el registro, la autorización de las transferencias internacionales de datos, promover la autorregulación, dictaminar sobre proyectos de disposiciones normativas, divulgar el contenido del derecho fundamental a la protección de datos, cooperar bilateral y multilateralmente con las autoridades de protección de datos.

En lo que hace a la promoción de la autorregulación por los órganos de control como instrumento complementario de protección de datos personales, esa promoción ha de representar un valor añadido —en su contenido— con respecto a lo que dispongan las leyes, debe contener o estar acompañado de elementos que permitan medir su nivel de eficacia en cuanto al cumplimiento y

al grado de protección de los datos personales, y debe consagrar medidas efectivas a ser aplicadas en caso de incumplimiento.

La Directriz 10, por su parte, consagra las sanciones para el caso de incumplimiento de las disposiciones que reflejen lo previsto en estas directrices. El sujeto legitimado para imponerlas es, o la autoridad de protección de datos, o el órgano judicial correspondiente. Las autoridades de protección de datos deberán tener capacidad suficiente para recurrir a las vías judiciales que resulten competentes para lograr la adopción de las medidas necesarias para garantizar el cumplimiento de estas directrices y, en particular, la imposición de las sanciones que correspondiesen. En el caso de que las autoridades de protección de datos fueran directamente competentes para la imposición de sanciones, sus resoluciones deberán ser recurribles ante los Tribunales de Justicia.

LA PROTECCIÓN DE DATOS EN EL URUGUAY DE HOY

MARCO NORMATIVO

La Constitución de la República

La Constitución uruguaya —siguiendo una tendencia que se repite en Iberoamérica— se afilia a la concepción jusnaturalista en materia de derechos fundamentales[31]. En este sentido, los artículos 72[32] y 332[33] vienen a marcar esta postura, en tanto reconocen la no taxatividad de los derechos constitucionales[34] y, por ende, admiten que la enumeración de derechos, deberes y garantías no excluye otros que son inherentes a la personalidad humana o se derivan de la forma republicana de gobierno[35].

Si bien no contiene consagración específica del derecho a la intimidad, en su artículo 7º, luego de enumerar el derecho de los habitantes de la República a ser protegidos en el goce de la vida, el honor, la libertad, la seguridad, el trabajo y la propiedad, estatuye "Nadie puede ser privado de estos derechos sino conforme a las leyes que se establecieren por razones de interés general".

Esta fórmula normativa del artículo 7º de la Constitución de la República opera la distinción de siete derechos fundamentales (libertad, vida, honor, seguridad, trabajo, propiedad), que la doctrina considera como derechos reconocidos por la Constitución, preexistentes a dicho cuerpo normativo y que son inherentes a todos los habitantes de la República como individuos de la especie humana, y una segunda clase de derechos consagrados constitucionalmente a favor del individuo, que básicamente constituyen el derecho a ser protegidos en el goce de cada uno de los derechos preexistentes, que nacen por la propia regulación que de los mismos hace el texto de nuestra Magna Carta y que las demás normas jurídicas precisan, reglamentan, garantizan.

Lo expresado viene a reafirmar la filiación jusnaturalista de nuestra Constitución, que no se

31 RISSO FERRAND, Martín J.. "*Control de la regularidad constitucional de las leyes que limitan o restringen derechos humanos en el derecho uruguayo*", Revista de Derecho III Universidad Católica Konrad Adenauer. Montevideo: Amalio Fernández, 2002, p. 59.

32 "La enumeración de derechos, deberes y garantías hechas por la Constitución, no excluye los otros que son inherentes a la personalidad humana o se derivan de la forma republicana de gobierno".

33 "Los preceptos de la presente Constitución que reconocen derechos a los individuos, así como los que atribuyen facultades e imponen deberes a las autoridades públicas, no dejarán de aplicarse por falta de la reglamentación respectiva, sino que esta será suplida, recurriendo a los fundamentos de leyes análogas, a los principios generales de derecho y a las doctrinas generalmente admitidas."

34 RISSO FERRAND, Martín J. "Derecho Constitucional", Tomo I, Fundación de Cultura Universitaria, Montevideo, 2005, p. 434.

35 REAL, Alberto Ramón. "Los principios generales de derecho como fuentes de derecho administrativo en el derecho positivo uruguayo". Montevideo: Fundación del Cultura Universitaria, 2001.

limita a crear derechos, sino que reconoce que existen derechos anteriores, que no requieren de ser creados normativamente.

Además, algunos artículos de la Constitución refieren a derechos fundamentales que son asociados al derecho de acceso y a la protección de datos personales. Los analizaremos a continuación.

En tal sentido, el artículo 10 inc. 1 de la Constitución de 1976 establece "Las acciones privadas de las personas que de ningún modo atacan al orden público ni perjudican a un tercero, están exentas de la autoridad de los magistrados", consagrando así la libertad de comunicación del pensamiento.

Por su parte, el artículo 28 establece "Los papeles de los particulares y su correspondencia epistolar, telegráfica o de cualquier otra especie, son inviolables, y nunca podrán hacerse su registro, examen o interceptación sino conforme a las leyes que se establecieren por razones de interés general".

A su vez, el artículo 29 expresa "Es enteramente libre en toda materia la comunicación de pensamientos por palabras, escritos privados o publicados en la prensa, o por cualquier forma de divulgación, sin necesidad de previa censura; quedando responsable el autor y, en su caso, el impresor o emisor, con arreglo a la ley por los abusos que cometieren".

En términos generales, en lo que hace a la normativa constitucional, habremos de concluir, indubitablemente, estableciendo que, aún a falta de disposición que expresamente regule la protección de datos personales o el habeas data, el amparo a nivel de nuestra Carta Mayor está presente y es adecuado tanto en lo que hace a su concepción jus naturalista de los derechos humanos, como en lo que concierne a la filosofía que inspira el articulado reseñado.

Por derechos humanos (derechos inherentes a la personalidad humana, también llamados esenciales o fundamentales[36]) entendemos aquellos derechos que tienen como sujeto al hombre en cuanto tal, en cuanto pertenece a la especie que llamamos humana, prescindiendo de su condición de ciudadano o extranjero de trabajador o pasivo, de niño, mujer o varón, de joven o anciano, de integrante de algún grupo étnico en especial o de toda otra circunstancia en particular[37].

Ante la necesidad de dar concreción a las disposiciones programáticas de nuestra Constitución que refieren a los principios generales del derecho y, en tanto tales comprenden al derecho fundamental a la protección de datos personales, adquiere relevancia el análisis de pactos, convenciones y declaraciones de carácter internacional que dan forma al instituto.

Normativa de carácter internacional

Entrando al análisis de la normativa de carácter internacional, sin pretensión de exhaustividad, mencionaremos tres cuerpos normativos, de los cuales dos, al haber sido ratificados parlamentariamente, se han constituido en ley en sentido material en nuestro país.

En primer lugar, el *Pacto Internacional de Derechos Civiles y Políticos*, que fuera aprobado por la Asamblea General de la Organización de las Naciones Unidas, en su Resolución 200 A (XXI) de 16 de diciembre de 1966, suscrita por Uruguay el 21 de febrero de 1967 y ratificada por Ley N° 13751, tiene pleno valor normativo.

En su artículo 17, establece "Nadie será objeto de injerencias arbitrarias o ilegales en su vida priva-

36 DURÁN MARTÍNEZ, Augusto. *"¿Se puede limitar derechos humanos por actos administrativos dictados por órganos reguladores de la actividad privada?*, Revista de Derecho III Universidad Católica Konrad Adenauer. Montevideo: Amalio Fernández, 2002, p. 170.

37 DURÁN MARTÍNEZ, Augusto. "*Estudios sobre derechos humanos*" Montevideo: Universidad Católica del Uruguay, Ingranusi Ltda., Montevideo, 1999.

da, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación", y continúa "Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques".

En segundo lugar, el *Pacto de San José de Costa Rica*, también conocido como *Convención Americana sobre Derechos Humanos*, que fuera ratificado por nuestro país por Ley N° 15.837, de 8 de marzo de 1985, en su artículo 11 establece "1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad; 2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación; 3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques", consagrando así el derecho a la privacidad y, también, el derecho del individuo a obtener información sobre su persona mediante el uso de los medios legales a su alcance.

En tercer lugar, la *Declaración Universal de los Derechos Humanos,* signada en Nueva York en la Asamblea General de las Naciones Unidas, el 10 de diciembre de 1948, en su artículo 12, establece "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques".

A su cita, corresponde la obligada pregunta acerca de cómo opera la incidencia de esta Declaración en el ámbito interno, puesto que no ha sido ratificada por nuestro país y este es un país de consagrada vocación romanista formalista. En efecto, la Declaración Universal no es un tratado, fue concebido en 1948 como la expresión de un ideal, como un modelo de inspiración para los textos constitucionales de los estados, pero hoy, cincuenta años después, como consecuencia de un complejo proceso jurídico político, en ella se basa el sistema de protección de los derechos humanos. "A pesar de no poseer carácter convencional, se considera como un instrumento del que resultan obligaciones jurídicas exigibles, como una verdadera fuente de derecho internacional"[38].

En tanto se trata de un documento con vocación universalista, la doctrina se ha encargado de fundamentar su obligatoriedad, sea recurriendo al concepto de costumbre internacional, a la luz de lo que es la práctica internacional, sea porque ha sido un documento concebido como un ideal común o como un instrumento a promover mediante la enseñanza y el respeto a los derechos y libertades.

La Declaración Universal de Derechos Humanos, en especial, se ha transformado a lo largo del tiempo en cita ineludible en materia de protección y respeto por los derechos humanos y constituye una declaración de principios generales de Derecho Internacional, que son una de las fuentes de derecho previstas por el Estatuto de la Corte Internacional de Justicia[39].

Mucho se ha hablado de la obligación de los estados de asegurar los niveles esenciales de los derechos, de cuáles son las técnicas de control más eficaces para la realización plena de los derechos civiles y políticos, y de los derechos económicos, sociales y culturales de los pueblos.

Los grandes tratados de derechos humanos de ONU[40] adoptaron técnicas como el examen de los informes que periódicamente los estados de-

38 GROS ESPIELL, Héctor, Montevideo: Colegio de Abogados del Uruguay, Tribuna del Abogado, 2003.

39 BLENGIO VALDÉS, Mariana. "*La Declaración Universal de Derechos Humanos como fuente de derecho*". Montevideo: Tribuna del Abogado, N° 125, nov.-dic.2001, p. 19 y sig.

40 A saber: Pacto Internacional de Derechos Civiles y Políticos, Convención Internacional sobre la Eliminación de todas las Formas de Discriminación Racial, Convención sobre la Eliminación de todas las Formas de Discriminación contra la Mujer, Convención contra la Tortura y otros Tratos o Penas Crueles, Inhumanos o Degradantes, Convención sobre los Derechos del Niño.

ben presentar a los Comités, y la competencia de estos para el dictado de Observaciones o Recomendaciones Generales, así como el régimen de comunicaciones individuales y el de comunicaciones por las que un estado alegue que otro estado Parte no cumple con sus obligaciones[41].

Doctrinariamente, ha surgido el principio de indivisibilidad o interdependencia de los derechos fundamentales, conforme el cual la plena realización de los derechos civiles y políticos sin el goce de los derechos económicos, sociales y culturales resulta imposible, pues la consecución de un progreso verdadero en la aplicación de los derechos humanos depende de buenas y eficaces políticas nacionales e internacionales de desarrollo económico y social[42], que ha sido reconocido en la Proclamación de Teherán de 1968, pretende llenar un vacío en lo que hace a la efectiva ejecución de los principios contenidos en tratados internacionales.

Otros instrumentos internacionales contienen recomendaciones y orientación en materia de protección de datos personales. Entre ellos podemos mencionar el Convenio 108 del Consejo de Europa, la Directiva 95/46/CE, la Recomendación de OCDE sobre circulación internacional de datos personales para la protección de la intimidad, adoptada el 23 de setiembre de 1980, la Resolución 45/95 de la Asamblea General de las Naciones Unidas, de 14 de diciembre de 1990.

41 GIALDINO, Ronaldo. "*Judicialidad de los derechos humanos, económicos, sociales y culturales*", *en "Derechos Humanos en situaciones de crisis en Uruguay*", publicación de las intervenciones del Seminario desarrollado en Montevideo los días 7 y 8 de octubre de 2002, organizado por Comisión de lucha contra la Corrupción, Uruguay Transparente, Asociación de Magistrados del Uruguay y Fundación Konrad Adenauer, pp. 127 y 128.

42 GIALDINO, Ronaldo. "*Judicialidad de los derechos humanos, económicos, sociales y culturales*", en "Derechos Humanos en situaciones de crisis en Uruguay". Publicación de las intervenciones del Seminario desarrollado en Montevideo los días 7 y 8 de octubre de 2002, organizado por Comisión de lucha contra la Corrupción, Uruguay Transparente, Asociación de Magistrados del Uruguay y Fundación Konrad Adenauer, p. 126.

En los hechos, la vaguedad de algunas normas contenidas en tratados, convenios o declaraciones de los estados, unida al hecho de que no existe unanimidad al interpretar dichas normas como garantizadoras de obligaciones de resultados (y no de medios) por parte de los Estados, nos enfrenta a serias dificultades a la hora de procurar la efectiva realización de los derechos en ellas contenidos. De ahí, la necesidad de concreta regulación en el derecho interno de los principios en ellos contenidos.

Normativa general

No existe en Uruguay una norma constitucional ni legal que tutele, con carácter general, la protección de datos personales.

No obstante ello, hemos sostenido que la Ley Nº 17.838, de 24 de setiembre de 2004, (Ley de Protección de Datos Personales para ser utilizados en informes comerciales y Acción de habeas data) contiene disposiciones de carácter general que refieren al tratamiento jurídico del tema, crea mecanismos administrativos tuitivos de la protección de datos personales en general y consagra la acción de habeas data.

Esta ley, en el decurso de su análisis legislativo, sufrió modificaciones que no le provocaron un cambio en su caratulación, no obstante lo cual le implicaron una clara ampliación de su objeto.

En efecto, además de regular específicamente lo atinente a los datos personales para informes comerciales, atribuye la competencia de órgano de control al Ministerio de Economía y Finanzas, analiza los principios generales en materia de protección de datos y consagra la acción jurisdiccional de habeas data a efectos de una debida tutela de los datos personales.

Explicita principios generales en la materia: legalidad, veracidad, adecuación, ecuanimidad, proporcionalidad, lealtad, uso reservado y acorde a la finalidad de la colecta, así como el derecho al olvido.

Al día de la fecha, transcurridos tres años desde la aprobación de la Ley N° 17.838, su reglamentación ha ido en el sentido de su aplicación con respecto a datos para ser utilizados en informes comerciales.

En tal sentido, la Comisión Consultiva de Protección de Datos Personales, dependiente del Ministerio de Economía y Finanzas, creada por imperio del artículo 20 de esta disposición normativa, en su cometido de asesoramiento en todas las acciones necesarias para el cumplimiento de los objetivos y disposiciones de la ley, ha declarado que su sistemática legal se aplica a todo tipo de datos (principios, derechos y acción de habeas data), pero en especial a la regulación del tratamiento de los datos personales destinados a brindar informes objetivos de tipo comercial, autorizados expresamente por los artículos 1º y 8º de la ley.

Por otra parte, el Decreto No. 396/006, de noviembre de 2006, reglamentó los artículos 1º, 13 y 20 de la ley No. 17.838, creando un registro de bases de datos, archivos, registros y otros medios similares autorizados, públicos o privados, destinados a brindar informes objetivos de carácter comercial y fijando un plazo de 90 días para la inscripción respectiva.

Conforme surge de su página web[43] se han efectuado las inscripciones de las empresas más importantes en el mercado uruguayo, destinadas a brindar informes de carácter comercial.

Normativa sectorial de carácter legal

Existe, en nuestro país, normativa aislada que tiene relación con la temática, que pasaremos a reseñar, en orden cronológico.

El Código Tributario *(Ley N° 14.306, de 29 de noviembre de 1974*) establece en su artículo 47 la obligación de los funcionarios de guardar secreto de las actuaciones.

La Ley Nº 14762, de 13 de febrero de 1978, que establece un nuevo sistema de identificación para las personas físicas, de las empresas y de los empresarios, en su artículo 21, estatuye que "Los datos que lleva la Dirección Nacional de Identificación Civil (Ministerio del Interior) son de carácter absolutamente reservados no pudiendo hacerse otro uso de ellos que el que autoriza expresamente la ley".

El secreto bancario ha sido instituido por el artículo 25 de la *Ley N° 15.322, de 17 de setiembre de 1982,* que fue objeto de interpretación legislativa con fecha reciente, el 13 de enero de 2006, al sancionarse la *Ley Nº 17.948,* que declara que el referido secreto profesional ampara exclusivamente las operaciones bancarias pasivas que realizan las instituciones de intermediación financiera y toda otra operación en la que estas asumen la condición de deudores, depositarios, mandatarios o custodios de dinero o de especie respecto de sus clientes, sin perjuicio del amparo de toda la información confidencial recibida del cliente comprendida también en la citada norma.

La *Ley N° 16.011, de 19 de diciembre de 1988,* tiene importancia en la materia, al consagrar la acción de amparo, pues es el mecanismo establecido por la ley como procedimiento judicial tuitivo de la protección de datos personales.

El ejercicio de la acción de amparo es viable si se dan los requisitos siguientes: a) acto, omisión o hecho, b) que en forma actual o inminente, c) lesione, altere o amenace, d) que tenga ilegitimidad manifiesta, e) que la afectación sea contra terceros, f) inexistencia de otros medios para promover el fin deseado. Consagra un medio rápido y sencillo para lograr la protección de los derechos humanos, como instrumento de protección genérica a la libertad informática, pero no consagra un procedimiento específico a seguir en los casos en los cuales una persona de-

43 http://www.mef.gub.uy/pdp.

see conocer los datos suyos que se encuentran en una base de datos y especifica "no podrán deducirse cuestiones previas" (artículo 12).

La *Ley N° 16.099, de 13 de noviembre de 1989*, también conocida como Ley de Prensa, viene a reglamentar la libertad de comunicación de pensamientos y de información, y a consagrar el derecho de respuesta de todos los ciudadanos aludidos en una publicación (u otro medio de comunicación pública). Establece un procedimiento oral y público, con asistencia obligatoria del juez a las audiencias, con plazos brevísimos y perentorios, la supresión de la prisión preventiva, la exclusiva jurisdicción ordinaria, el perfeccionamiento del derecho de respuesta y la fortificación de la posición procesal del ofendido [44].

La *Ley N° 16.616, de 20 de octubre de 1994*, conocida como Ley de Sistema Estadístico Nacional, en su artículo 3º establece "Los organismos que integran el Sistema Estadístico Nacional deben servir con objetividad los fines de su creación con sometimiento pleno al Derecho y deben actuar de acuerdo con los siguientes principios generales: secreto estadístico, pertinencia, transparencia, rigurosidad, autonomía técnica, comparabilidad, eficiencia, centralización normativa, descentralización operativa, legalidad objetiva y motivación de la decisión".

El *artículo 694 de la Ley N° 16.736*, de 6 de enero de 1996, regula el pleno acceso a la información de interés, en los siguientes términos: "Las Administraciones públicas impulsarán el empleo y aplicación de medios informáticos y telemáticos para el desarrollo de sus actividades y el ejercicio de sus competencias, garantizando a los administrados el pleno acceso a las informaciones de su interés".

Para los funcionarios del Banco de Previsión Social rige lo dispuesto en el Código Tributario, modificado por las leyes *N° 16790 y N° 16713*, que regulan el acceso a los registros de la historia laboral.

El Código de la Niñez y la Adolescencia, aprobado por *Ley Nº 17823, de 7 de setiembre de 2004*, en sus artículos 218 y siguientes refiere a los datos personales de los menores contenidos en el Sistema Nacional de Información sobre Niñez y Adolescencia, que se crea por imperio de esta disposición normativa.

Su artículo 221, en tal sentido, establece "se deberá garantizar el uso reservado y confidencial de los datos correspondientes a cada niño o adolescente, en concordancia con su interés superior y en cumplimiento del derecho a la privacidad de su historia laboral, como único propietario de la misma".

Y el 222 establece "los antecedentes judiciales y administrativos de los niños o adolescentes que hayan estado en conflicto con la ley se deberán destruir en forma inmediata al cumplir los dieciocho años o al cese de la medida".

La *Ley Nº 17835, de 23 de setiembre de 2004*, determina las limitaciones a las disposiciones sobre secreto, en los términos que siguen: "Todas las personas físicas o jurídicas sujetas al control del Banco Central del Uruguay estarán obligadas a informar las transacciones que, en los usos y costumbres de la respectiva actividad, resulten inusuales, se presenten sin justificación económica o legal evidente, o se planteen con una complejidad inusitada o injustificada, así como también las transacciones financieras que involucren activos sobre cuya procedencia existan sospechas de ilicitud, a fin de prevenir el delito de lavado de activos".

La *Ley Nº 17930, de 19 de diciembre de 2005*, por su parte, contiene varias disposiciones que hacen a la protección de datos personales.

44 VALDES COSTA, Ramón. "*Libertad de comunicación de pensamientos y de informaciones en el derecho uruguayo*", Montevideo: trabajo inédito presentado en la Facultad de Derecho de la Universidad de la República, mayo de 1990.

Su artículo 261 establece la prohibición de "cesión, venta, reproducción, entrega a terceros de la información relativa al estado civil de las personas por quienes reciben la misma en virtud de convenios celebrados con la Dirección General del Registro de Estado Civil, sean personas físicas o jurídicas, públicas o privadas, y se realice en forma onerosa o gratuita. La misma prohibición alcanzará a aquellos que reciban por cualquier otro medio, directo o indirecto, información concerniente al estado civil de las personas cuyo registro, conservación y expedición es cometido de la Dirección General del Registro de Estado Civil. La Dirección General del Estado Civil será la encargada de fiscalizar el cumplimiento de lo establecido en este artículo. El Ministerio de Educación y Cultura reglamentará las sanciones económicas a aplicar ante el incumplimiento de la prohibición establecida".

Su artículo 320 edicta "Créase en la órbita de la Inspección del Trabajo y la Seguridad Social el Registro de Empresas Infractoras, que funcionará de acuerdo a la reglamentación que dicte el Poder Ejecutivo".

Su artículo 469 consagra la obligación de todos los órganos u organismos públicos estatales o no estatales de "aportar sin contraprestación alguna, los datos que no se encuentren amparados por el secreto bancario, estadístico y que le sean requeridos por escrito por la Dirección General Impositiva para el control de los tributos", eximiendo de esta obligación al Poder Judicial y al Poder Legislativo, cuando se tratase de datos o documentos correspondientes a actuaciones de carácter reservado o secreto. Procura, de esta forma, evitar la evasión fiscal controlando los datos personales contenidos en bases de datos —así se trate de bases de datos públicas o privadas— de naturaleza diversa, datos que fueron recabados para finalidades diferentes de las que inspira esta norma. Pune el incumplimiento con multa. Declara que la información recibida quedará amparada por el secreto que rige los procedimientos tributarios.

La *Ley Nº 17948, de 13 de enero de 2006,* en su artículo 2º declara que toda persona, física o jurídica, podrá solicitar información acerca de cualquier persona física o jurídica y del conjunto económico que esta persona integre en su caso, que opere con instituciones de intermediación financiera, concerniente a las operaciones bancarias activas y a su categorización o rango de riesgo crediticio asignado, que conste en la Central de Riesgos Crediticios que lleva actualmente el Banco Central del Uruguay, con las limitaciones que hacen a la confidencialidad en los términos de la Ley Nº 15322. Asimismo, en su artículo 3º faculta al BCU a divulgar dicha información y establece en qué términos deberá realizar la comunicación.

La *Ley Nº 17957, de 18 de abril de 2006,* crea el Registro de Deudores Alimentarios morosos en la órbita de la Dirección General de Registros, Registro Nacional de Actos Personales, Sección Interdicciones.

Nuestro *Código Penal*, en sus artículos 296 y siguientes, tipifica los delitos de violación de correspondencia, interceptación de noticia, revelación de correspondencia, conocimiento fraudulento de documentos secretos, revelación de documentos secretos.

Decretos

En lo que refiere a problemas que pudieran surgir con relación a datos médicos, el *decreto N° 258/992* regula las obligaciones del médico con relación a los registros, el derecho a la intimidad del paciente, así como su derecho a la información.

El *decreto Nº 204/001* amplía el ámbito de validez del decreto anteriormente mencionado, que circunscribía su eficacia a los hospitales dependientes del Ministerio de Salud Pública, dándole validez general a los preceptos en él contenidos.

El *decreto Nº 396/003, de 20 de setiembre de 2003,* crea el sistema de historia clínica electró-

nica única para cada persona, y establece que deberá ajustarse a los principios generales de finalidad, veracidad, confidencialidad, accesibilidad y titularidad particular.

Por su parte, en el análisis del expediente electrónico, el *decreto N° 65/98, de 10 de marzo de 1998*, se prevé que es falta gravísima la divulgación de la contraseña del funcionario autorizado, aún si no llega a ser usada.

Más recientemente fueron aprobados los *decretos N° 249/2007 y N° 250/2007, de 9 de julio de 2007*, que instituyen un sistema de identificación de las personas físicas en base a asignar un número de cédula de identidad desde el momento mismo del nacimiento, que quedará incluido en el certificado médico de nacimiento y en las actas de nacimiento de la Dirección General del Registro de Estado Civil. La expedición del "certificado de nacido vivo" será un producto de labor coordinada entre la Dirección de Identificación Civil del Ministerio del Interior, la Dirección General del Registro de Estado Civil del Ministerio de Educación y Cultura, y el Ministerio de Salud Pública. En la implementación práctica del sistema, se creó un grupo de trabajo en el que tienen injerencia —además de los mencionados— la Oficina de Planeamiento y Presupuesto (Presidencia de la República), cuyo Director le presidirá, el Director Técnico del Instituto Nacional de Estadística (Presidencia de la República), el Director General de la Salud (Ministerio de Salud Pública), el Presidente del Banco de Previsión Social , un representante de la Agencia para el Desarrollo del Gobierno Electrónico (Presidencia de la República) y un representante del Ministerio de Desarrollo Social.

Acordada

Por Circular nº 8/2006, la Suprema Corte de Justicia comunicó el texto de la Acordada nº 7564, de 10 de febrero de 2006, que procura el equilibrio en la protección en el goce de derechos fundamentales, el derecho a la información y la tutela del derecho a la intimidad (Considerando II), y tiene por objeto la protección integral de los datos personales asentados en bancos o bases de datos documentales o jurisprudenciales en el Poder Judicial (artículo 1º).

Posteriormente, por Circular No. 115/2006, en consideración a las diferencias y dificultades surgidas con motivo de la interpretación y aplicación de la Acordada antes reseñada, por la Acordada No. 7578, se suspendió la vigencia de la Acordada No. 7564, y se integró una Comisión a efectos de proceder a revisar su texto de modo de contemplar y armonizar adecuadamente los diversos principios, derechos e intereses involucrados.

EL SISTEMA LEGAL EN PROTECCIÓN DE DATOS PERSONALES

El modelo uruguayo nos muestra, por un lado, normativa marco, constituida por las disposiciones de los artículos 72 y 332 de la Constitución de la República (1967), que consagran los principios generales como fuente de derecho en nuestro país. Esta concepción —jusnaturalista— nos habilita a decir que no existe desamparo para los ciudadanos uruguayos, y que sus datos personales tienen medios de protección consagrados en la Carta. La interpretación de nuestra Constitución en su carácter de normativa enmarcadora de los principios generales del derecho nos permite una interpretación de los principios consagrados en tratados internacionales como parte integrante del ordenamiento jurídico nacional. Entendemos, por tanto, que la protección de datos personales está implícitamente consagrada en nuestro ordenamiento jurídico normativo con carácter general.

Además, en nuestro país, existe expresa consagración normativa por medio de lo que podemos denominar "familias de normas", cuyo contenido hemos analizado más arriba, que vienen a regular

distintos aspectos que conciernen a la protección de datos personales y al derecho de acceso. Así: el secreto tributario y previsional (leyes N° 14305, N° 16790, N° 16713), el secreto bancario (artículo 25 de la Ley N° 15322 y Ley N° 17835), el secreto estadístico (Ley N° 16616), el derecho de acceso a la información (artículo 694 de la Ley N° 16736), el acceso por la autoridad impositiva a los datos que se encuentren en poder de órganos u organismos públicos estatales o no estatales para el control de los tributos (artículo 469 de la Ley N° 17930), la acción de amparo (Ley N° 16099), la protección de los datos de identificación civil (artículo 21 de la Ley N° 14762, decretos n° 249 y n° 250 de 2007), la prohibición de cesión, venta, reproducción o entrega a terceros de información relativa al estado civil de las personas del Registro de Estado Civil (artículo 261 de la Ley N° 17930); la inscripción registral de las personas que tienen la condición de deudor alimentario moroso (Ley N° 17957), el carácter reservado de los datos personales de los menores y adolescentes (artículos 218 y siguientes del Código de la Niñez y la Adolescencia), los datos médicos (decretos n° 258/992, n° 204/001, n° 396/003), la consagración de la libertad de pensamientos e información (Ley N° 16099), el sector comercial (Ley N° 17838), la acción de habeas data (Ley N° 17838), la creación de un Registro de Empresas Infractoras a la normativa laboral en la órbita del Ministerio de Trabajo y Seguridad Social (artículo 320 de la Ley N° 17930).

De lo cual podemos inferir que, si bien nuestra Constitución no ampara explícitamente la protección de datos personales ni el acceso a la información como derechos fundamentales, no puede concluirse que nuestro ordenamiento no posea medios para la tutela de los datos personales. Sí los posee en función de los preceptos constitucionales, que habrán de ser informados conjuntamente con los contenidos de las declaraciones y convenios multilaterales signados por nuestro país, y la variada y dispersa normativa existente.

El sistema uruguayo de protección de datos, aún sin contener una ley que ampare con carácter general la protección de los datos personales, sí posee una adecuada enumeración y desarrollo de los principios generales que rigen el derecho fundamental a la protección de datos personales (Ley N° 17838, Ley N° 16616), tiene expresa consideración del derecho de acceso (Ley N° 16736), define los datos sensibles (Ley N° 17838), tiene consagrada la acción de amparo como instrumento procesal para el ejercicio de los derechos de acceso, rectificación, corrección de los datos (Ley N° 17838, Ley N° 16099).

Los derechos de los titulares de los datos, así como también las obligaciones y responsabilidades de los custodios de los datos lucen consagradas en los distintos casos de regulación sectorial mencionados, al igual que los principios que son enumerados a título ejemplificativo.

Prima el principio del consentimiento, que ha sido consagrado con carácter general en la Ley N° 17838, conforme el cual la determinación de qué hacer y qué no hacer con los datos corresponde a su titular y no a quien realiza la colecta, o los coloca en un registro, y es su titular quien puede disponer de ellos. Este principio puede ser relevado mediante una ley, dictada por razones de interés general (artículos 4 y 8 de la Ley N° 17838).

En términos generales, el sistema uruguayo nos brinda algunas herramientas para la protección de los datos, que no son pocas.

La legislación, hoy por hoy, ha ido marcando la tendencia de propiciar un más generalizado y más económico acceso al crédito, obviando la requisitoria del consentimiento y facilitando el ejercicio del derecho de acceso a la información, la libertad de opinión y la libertad de información, y procurando por este medio la mayor facilitación del comercio. En este sentido nuestro legislador ha aprobado sendos cuerpos normativos, para los datos comerciales la Ley N° 17838 (24 de setiembre de 2004), para delimitar el

concepto de secreto bancario la Ley N° 17948 (13 de enero de 2006).

Esta tendencia tomó forma luego de operada la crisis bancaria del 2002, y tiene su razón de ser en la necesidad del fomento del crédito. Permite que, cuando vamos a solicitar un préstamo o una hipoteca, se nos soliciten datos sobre los bienes que poseemos, si la propiedad donde vivimos es alquilada o propia, nuestro sueldo, ingresos del núcleo familiar, número de hijos, datos que son de utilidad para definir el perfil socio económico y en definitiva conceder o no el préstamo o el servicio financiero de que se trate[45]. Colaboran a definir el riesgo que puede existir en la concesión de un préstamo, lo que permite —en definitiva— conceder préstamos a valores más accesibles cuando el riesgo es menor.

Ahora bien, en el mismo sentido el 13 de enero de 2006 ha quedado aprobada la Ley N° 17948, que otorga el carácter de información de acceso público a la información sobre deudores del sistema financiero incorporados a la Central de Riesgos Crediticios que lleva la Superintendencia de Instituciones de Intermediación Financiera y habilita que esta sea accedida por "toda persona física o jurídica", sin exigir un interés determinado que califique a la persona.

Esta tendencia a la apertura de la información bancocentralista sigue los lineamientos que pueden apreciarse en el sistema argentino y en el español, aunque no se aprecian en el régimen uruguayo limitaciones al acceso, que habrán de surgir de la reglamentación de dicho texto normativo.

Asimismo, resulta importante a efectos de que los ciudadanos vean respetados en forma sus derechos, que la reglamentación de la Ley N° 17948 tenga en consideración que el acceso debe ser calificado, y que deben respetarse los principios que informan la protección de los datos personales, en especial el principio de finalidad, de calidad de los datos, de proporcionalidad, veracidad, pertinencia, exactitud, adecuación, seguridad. En tal sentido, la aplicación del principio de transparencia cumplirá su cometido cabalmente sólo si se respetan los derechos y las garantías de los ciudadanos.

Tanto el derecho a la protección de datos personales como el derecho a la información, no son derechos absolutos, sino que son derechos fundamentales, y llegado el caso habrá que evaluar, cuándo entran en juego otros derechos y este principio admite excepciones[46]. Es aquí donde entra a regir la ponderación de los distintos derechos que, siendo de jerarquía similar, que habrá de aplicarse puesto que ambos derechos deben coexistir en equilibrio[47].

Hemos apreciado también la tendencia hacia un mayor control de la información, que tiende a centralizarse. Así, se ha creado un Registro de Deudores Alimenticios Morosos en la Dirección de Registros (Ley N° 17957, de 17 de abril de 2006), un Registro de Empresas Infractoras en el Ministerio de Trabajo y Seguridad Social (Ley N° 17930, de 19 de diciembre de 2005), se ha consagrado la obligación de todos los organismos estatales o no estatales —con la única excepción del Poder Judicial y el Poder Legislativo— de aportar datos a los efectos del control de la recaudación tributaria (Ley N° 17930, de 19 de diciembre de 2005).

45 FERNANDEZ, Eduardo (2004). "L*a perspectiva de la Asociación de Empleados Bancarios del Uruguay*" en "*Seguridad, privacidad, confidencialidad. El desafío de la Protección de Datos*". Ed. Trilce, Montevideo, p. 56.

46 SUÑE, Emilio (2002). "*Tratado de Derecho Informátic*o", Vol. I , 2ª ed. Madrid, 2002 p. 83

47 SUPREMA CORTE DE JUSTICIA DE URUGUAY "Ahora bien, la libertad de información, tanto de recibirla como de difundirla no es un derecho absoluto, en tanto conviva con otros derechos constitucionales entre los cuales se encuentran los llamados derechos a la personalidad, como lo son el derecho a la integridad moral, al honor, a la imagen, a la intimidad de las personas" (sentencias N° 25/1996, N° 253/1999).

Al respecto, la tendencia legislativa es a propiciar un mayor control por parte de las autoridades del estado de la información sobre los ciudadanos, propiciando la transparencia de los datos contenidos en estos registros.

Ahora bien, en estos casos, por disposición de una ley fundada en razones de interés general, se determinó que no es necesario el consentimiento del titular a efectos de sus datos sean incorporados en los registros o base de datos mencionados. Esto no obsta a que el derecho a la protección de los datos que están siendo objeto de registro o consulta sea respetado: el titular de los datos tiene derecho a que la recolección de su datos sea realizada adecuadamente, que el procesamiento de los mismos se efectúe con calidad, precisión, que la finalidad para la cual el dato es recogido sea respetada, especificada y limitada, que el dato sea brindado proporcionalmente con la función de transparencia que viene a cumplir. A su vez, el titular de los datos habrá de tener derecho a participar en el control de la veracidad de lo que a él concierne, habrá de tener derecho de acceso a los registros de sus datos, en definitiva, habrá de asegurársele el tratamiento en forma de sus datos. El o las personas responsables del registro o base de datos habrán de cumplir con los requisitos que le sean exigidos a efectos de salvaguardar la seguridad de los datos y sobre la forma de proveer seguridad habrá de informar a todo quien correspondiera. Todos estos requisitos son normalmente objeto de control por una autoridad, que ejerce la supervisión de que sean respetados los principios en materia de protección de datos, que habrá de funcionar con autonomía y en forma independiente de los organismos que tienen a su cargo la colecta y organización de los datos.

Algunas disposiciones sectoriales han creado autoridades de control de los datos, como es el caso del Instituto del Niño y el Adolescente para los datos contenidos en sus archivos, o del Ministerio de Economía y Finanzas para los datos de carácter comercial.

No obstante ello, entendemos que es prioritaria la creación de una autoridad de control que, con carácter general, con vocación autónoma y con independencia de los órganos que llevan los registros, pueda priorizar los derechos de los ciudadanos con respecto a sus datos personales, sea que estén contenidos en archivos informatizados o manuales, públicos o privados.

PROYECCIONES DE REFORMA

A estudio del parlamento se encuentran al día de la fecha dos proyectos de ley que pueden delinear próximos cambios en el sistema de protección de datos uruguayo. El primero, sobre "Acceso a la información pública y amparo informativo e Instituto Nacional para la información pública", se encuentra a estudio de la Comisión de Educación y Cultura de la Cámara de Senadores desde el año 2006 (Carpeta N° 541/2006). El segundo, sobre protección de datos, ingresó desde el Poder Ejecutivo al análisis del Poder Legislativo en este mes de septiembre de 2007, se le dará ingreso formal a la Cámara de Senadores en la primera sesión de octubre y, según nos fuera informado, pasará a ser analizado por la Comisión de Constitución y Legislación de esta Cámara parlamentaria uruguaya.

CONCLUSIONES

Cómo evaluar el sistema legal uruguayo en materia de protección de datos personales?

Pues si se trata de evaluar el grado de conformidad de los ciudadanos por la cantidad de acciones incoadas para proteger sus datos personales o acceder a la información, podemos observar que la cantidad de acciones incoadas es mínimo, por lo cual deberíamos concluir que el sistema funciona más que fluidamente.

Ahora bien, este parámetro no siempre se presenta como un parámetro adecuado, en mérito a las consideraciones que formularemos más adelante.

En primer lugar, el parámetro no es correcto porque el ciudadano medio uruguayo no posee el grado necesario de información para adquirir conciencia del riesgo que corre si no realiza un adecuado control —personal y concienzudo— de quién recaba sus datos, con qué finalidad, con quién serán compartidos, cómo se aseguran estos datos frente a terceros, quién será responsable de su seguridad.

Sólo un ciudadano bien informado puede realizar tales controles.

De la protección de datos se ha dicho que es como un rayo de sol en las sociedades democráticas, que trasvasa varias capas de la sociedad y del orden jurídico político impuesto al ciudadano para la vida en sociedad. Un funcionamiento defectuoso de la protección nos muestra que hay deficiencias en el sistema, que pueden ser consecuencia de que no exista un buen nivel de información en el ciudadano que por tanto no ejerce en forma sus derechos, puede ser consecuencia de que este ciudadano no posea los medios (jurídicos, económicos) para el ejercicio de tales derechos, puede ser consecuencia de que este ciudadano no se sienta seguro de que al intentar ejercer sus derechos pueda ser discriminado arbitrariamente. Ahora bien, un buen funcionamiento del sistema de protección de los datos que conforme a los ciudadanos y los mantenga informados, nos muestra una sociedad democrática sana, en que los ciudadanos pueden ejercitar sus derechos fundamentales y no se verán violentados en su ejercicio.

A partir del 11 de setiembre de 2001 hemos asistido a un proceso en que el valor seguridad ha tomado un lugar predominante. A efectos de combatir la criminalidad, el terrorismo, la violencia, los ciudadanos tienden a exigir que el estado cumpla con especial énfasis su función de vigilancia, y a colocar todos sus datos personales a disposición siempre que el tal cometido sea ejercido con eficacia. El estado, por consecuencia, se muestra ávido por recabar los datos de sus ciudadanos, otorgando preminencia al valor seguridad. A su vez, la facilidad y la economía con que las nuevas tecnologías permiten el tratamiento de la información en formas rápidas y confiables, han generado una tendencia cada vez mayor a la colecta de los datos de los ciudadanos, que ven sus actividades cotidianas reflejadas en bases de datos que operan facilitando la interacción comercial.

Algunos autores[48] refieren a esta situación en que se ve inmerso el ciudadano, cuyos datos son colectados por el estado y también por las empresas, como "el abrazo invisible" que proveen los intereses convergentes de estado y empresas a los ciudadanos, "abrazo" que constituye una verdadera amenaza para los derechos individuales y humanos en general, que pueden verse oprimidos por el "abrazo" hasta desaparecer.

Se ha hablado de una sociedad en que queda poco espacio para que los ciudadanos puedan desarrollar su individualidad, y ese espacio se encuentra solamente en aquellos ámbitos donde

48 EIKIN-KOREN, Niva, BIRNHACK, Michael D. "*Securing rights in a messy legal regime*" (2004). Trabajo inédito presentado en Stanford Law School, Stanford Program on Law Science and Technology.

ni el estado, ni las empresas comerciales, tienen interés en introducir su operativa.

Es así como podemos observar que los derechos y garantías individuales se van transformando en letra muerta: Muchos ciudadanos, ante el temor de ejercer sus derechos y que esto tenga por consecuencia una estigmatización de su persona por parte del estado, simplemente no los ejercen.

Es entonces cuando nos preguntamos si el ciudadano uruguayo tiene la perspectiva para encarar la protección de sus datos, o en qué medida es consciente de su papel en la defensa de sus intereses.

Si el ciudadano no tiene posibilidades reales de controlar quién accede a sus datos, para qué y bajo qué condiciones, la posibilidad de ejercer en forma sus derechos fundamentales es muy escasa. Por otro lado, las posibilidades de que sus datos sean manipulados de mala fe se acrecientan si no se le otorgan los medios necesarios para encarar su rol social.

Este peligro es aún mayor cuando el estado o los particulares tienen tecnológicamente la posibilidad de conformar perfiles de los ciudadanos, utilizando medios informáticos que comparan datos y unifican datos personales para coadyuvar a poseer información acerca de costumbres, prácticas, aspiraciones, enfermedades, tendencias políticas o sexuales, estudios de las personas. El cotejo de estos datos realizado por medios informáticos no siempre arrojará resultados ajustados a la realidad, sea quien fuere que los realice, puede estar errado por simple falta de diligencia, o por manipulación, o porque no se realizaron los controles necesarios para que el cotejo otorgue las garantías necesarias.

Por esa razón es que no hemos de hablar de datos sin dar al tema la debida relevancia.

El derecho a la protección de los uruguayos frente al procesamiento de sus datos personales surge ante la necesidad de reflexionar sobre los avances de la tecnología y sobre su influencia en la conformación práctica de sus derechos y libertades. El ciudadano uruguayo debe sentir que —ante los avances invasivos de la tecnología— su dignidad está siendo protegida jurídica y socialmente, que posee un acceso libre a la información que le concierne, que se tutela a la persona frente al procesamiento de sus datos personales. La protección de datos, por tanto, emerge como un presupuesto previo y necesario para cumplimentar en forma las exigencias de vivir en estado de derecho. El control que realiza cada ciudadano sobre sus datos aparece como condición esencial para una convivencia política en democracia.

Para ello, es menester que tengamos ciudadanos uruguayos muy conscientes de los riesgos en que pueden incurrir por no ejercer en forma la protección de sus datos.

Ahora bien, quién controla que el ciudadano posea un adecuado control sobre sus datos personales? Quién puede tener a su cargo el control de que los uruguayos tengamos acceso a los datos de que somos titulares? Quién controla que los uruguayos posean la necesaria capacidad de intervención ante la manipulación de sus datos por terceros?

Los diversos regímenes jurídicos que operan en el mundo nos muestran diversas formas de ejercer este control. Si la tendencia es hacia el mayor acopio de datos por parte del Estado, no ha de estar el control exclusivamente a su cargo, si es hacia el acopio con fines de marketing no habrá de estar en manos de grupos de interés comercial. En algunos países la misma autoridad controla el acceso y la protección del dato (Alemania), en otros países hay autoridades especializadas en la protección de los datos personales (España). El control es necesario en todas las etapas: colecta del dato, el almacenamiento, el tratamiento, todas estas instancias habrán de ser objeto de control, de análisis y de autorización

por la autoridad de control, que ejercerá su "imperium" sobre todos los datos que se encuentren en archivos o bases de datos públicas y privadas. El rasgo que no puede faltar en una autoridad de control es el de la independencia técnica, sólo en esas premisas puede actuar competencia, y con efectividad. Tanto el contralor preventivo, como el contralor que se ejerce sobre el tratamiento del dato y la finalidad para la que fue recabado, como todo el proceso que implica concientizar e informar a la ciudadanía, habrán de tener posibilidad de incidir en proceso de trasmisión de los datos. Sólo así no será posible que los datos se transformen en bienes de mercado, que puedan ser ofrecidos al mejor postor, o que se constituyan en factores de dominación de aquellos que son socialmente más poderosos.

Con relación a nuestro país, en razón de lo expuesto, hemos de concluir que el sistema uruguayo de protección de datos personales es incompleto y no se adapta fielmente a ninguno de los modelos que analizamos en el presente trabajo. El cotejo del sistema uruguayo con el que se propugna desde las Directivas aprobadas en Cartagena de Indias, es muy ilustrativo al respecto. Muchas son las cuestiones pendientes de mejorar: la concienciación de la ciudadanía uruguaya es muy baja, la creación de una ley de protección de datos con carácter general surge como una necesidad latente, la necesidad de una figura jurídica que provea al respecto en carácter de autoridad de control parece inminente. Es mucho lo que queda por hacer para que Uruguay logre obtener un nivel acabado de protección de datos. Este ha de ser nuestro reto en los próximos años...

BIBLIOGRAFÍA

ARGÜELLO TÉLLEZ, Fernando (2003). "*Protección de datos personales: la Directiva Comunitaria, su influencia y repercusiones en Latinoamérica*". En: Protección de Datos de Carácter Personal en Iberoamérica. Tirant lo Blanch. Valencia, España, 2005.

BARTH JIMENEZ, José Francisco (2003) "*Marco normativo y jurisprudencial de la protección de datos en Costa Rica*". En: Protección de datos de carácter personal en Iberoamérica. Ed. Tirant lo Blanch, Valencia, España, 2005.

BLENGIO VALDÉS, Mariana (2001). "*La Declaración Universal de Derechos Humanos como fuente de derecho*". En: Tribuna del Abogado, N° 125. Montevideo, Uruguay.

BRAUSE, Alberto (2003). "*Situación en Uruguay sobre la Protección de Datos Personales*". En: Protección de Datos de Carácter Personal en Iberoamérica. Tirant lo Blanch, Valencia, España, 2005.

CHIRINO, Alfredo y CARVAJAL PÉREZ, Marvin (2003). En: "*Protección de Datos de Carácter Personal en Iberoamérica* ", Tirant lo Blanch, Valencia, España, 2005.

CORREA FLEITAS, Ruben. "*Habeas Data Ley N° 17.838 de 24 de setiembre de 2004*". En: La Justicia Uruguaya. Tomo 131, accesible desde http://www.lju.com.uy.

CHESBRO, Michael E. (1999) "*Privacy for sale. How Big Brother and Others Are Selling Your Private Secrets for Profit*" Paladin Press. Bouder, Colorado, Estados Unidos de Norteamérica.

DELPIAZZO, Carlos E. (2001). "*Dignidad Humana y Derecho* ", Facultad de Derecho de la Universidad de Montevideo, Montevideo, Uruguay.

_____, (2004). "*Primera lectura de la Ley N° 17.838 de 24 de setiembre de 2004*". En: Anuario de Derecho Informático, Tomo V, Fundación de Cultura Universitaria, Montevideo, Uruguay.

_____, (2004). "*Estado de Protección de datos personales en Uruguay*". En: Anuario de Derecho Informático, Tomo IV, Fundación de Cultura Universitaria, Montevideo, Uruguay.

_____, PASCALE, Maricarmen y otros (2005). "*Protección de datos personales en Uruguay y el Mercosur*". Fundación de Cultura Universitaria, Montevideo, Uruguay.

DURÁN MARTÍNEZ, Augusto (2002). "*¿Se puede limitar derechos humanos por actos administrativos dictados por órganos reguladores de la actividad privada*? En: Revista de Derecho III, Universidad Católica Dámaso Antonio Larrañaga, Konrad Adenauer. Amalio Fernández, Montevideo, Uruguay.

_____, (1999) "*Estudios sobre derechos humanos*", Universidad Católica del Uruguay, Ingranusi Ltda., Montevideo, Uruguay.

FERNANDÉZ, Eduardo (2004). "*La perspectiva de la Asociación de Empleados Bancarios del Uruguay*". En: "¿Seguridad, Privacidad, Confidencialidad? El desafío de la protección de datos personales". Edición Trilce, Montevideo, Uruguay.

GIALDINO, Ronaldo (2002). "*Judicialidad de los derechos humanos, económicos, sociales y culturales*". En: "Derechos Humanos en situaciones de crisis en Uruguay", publicación de las intervenciones del Seminario desarrollado en Montevideo, organizado por Comisión de lucha contra la Corrupción, Uruguay Transparente, Asociación de Magistrados del Uruguay y Fundación Konrad Adenauer. Montevideo, Uruguay.

GROS ESPIELL, Héctor, Montevideo (2003). En Tribuna del Abogado. Colegio de Abogados del Uruguay, Montevideo, Uruguay.

GUTIÉRREZ CARRAU, Juan Manuel y otros (2005). "*Datos Personales para Informes Comerciales y Habeas Data*", BID —Liga de Defensa Comercial— Universidad de Montevideo, Montevideo, Uruguay.

MARABOTTO LUGANO, Jorge y otro (1998). "*Protección de datos personales y garantías constitucionales*". En: Tomo de ponencias de VI Congreso Iberoamericano de Derecho e Informática, Montevideo, Uruguay.

Instituto de Derecho Informático. Opinión Consultiva: "*Proyecto de ley sobre datos personales para informes comerciales y derecho de habeas data*" (2004). En: Anuario de Derecho Informático Tomo IV, Fundación de Cultura Universitaria, Montevideo, Uruguay.

PEÑA, Miguel Ángel (2004). "*La responsabilidad de los medios de comunicación en Internet*". En: Anuario de Derecho Informático, Tomo IV. Fundación de Cultura Universitaria, Montevideo, Uruguay.

PÉREZ LUÑO, Antonio Enrique. "*Derechos humanos, estado de derecho y constitución*", 3ª. Ed., Editorial Tecnos, Madrid, España.

RISSO FERRAND, Martín J. (2002) "*Control de la regularidad constitucional de las leyes que limitan o restringen derechos humanos en el derecho uruguayo*". En: Revista de Derecho III Universidad Católica Konrad Adenauer. Ed. Amalio Fernández, Montevideo, Uruguay.

_____, (2005) "*Derecho Constitucional*", Tomo I, Fundación de Cultura Universitaria, Montevideo, Uruguay.

REAL, Alberto Ramón. (2001) "*Los principios generales de derecho como fuentes de derecho administrativo en el derecho positivo uruguayo*". Fundación del Cultura Universitaria, Montevideo, Uruguay.

SWIRE, Peter P. y BERMANN, Sol (2007). "*Information Privacy. Official Reference for the Certified Information Privacy Professional (CIPP)".* International Association of Privacy Professionals (IAPP). York, Maine, Estados Unidos de Norteamérica.

VALDES COSTA, Ramón. (1990) "*Libertad de comunicación de pensamientos y de informaciones en el derecho uruguayo*". Trabajo inédito presentado en la Facultad de Derecho de la Universidad de la República, Montevideo, Uruguay.

http://www.mef.gub.uy/pdp

Declaración de Montreux (2005). "*La protección de datos personales y de la intimidad en un mundo globalizado: un derecho universal que respeta diversidades*", Reunión Anual de Comisionados de Protección de Datos, Conclusión 17: Enumeración de principios. (La traducción nos pertenece), Montreux, Suiza.

Dictamen 4/2002, de adecuación de la República Argentina a la Directiva 95/46/CE, emitido por el Grupo de Trabajo del artículo 29.

Declaración de La Antigua, numeral 7º.

Declaración de Santa Cruz de la Sierra, numeral 45.

Declaración de Santa Cruz de la Sierra, numeral 45.