APROXIMACIÓN A LA LEY URUGUAYA Nº 17.838
SOBRE PROTECCIÓN DE DATOS PERSONALES Y HABEAS DATA

Carlos E. Delpiazzo
Doctor en Derecho y Ciencias Sociales,
Director del Instituto de Derecho Informático,
Universidad Mayor de la República Oriental del Uruguay.

SUMARIO: I.- INTRODUCCIÓN. Aproximación a la ley Nº 17.838 desde cinco enfoques.- II.- ENFOQUE CONCEPTUAL. Del derecho a la intimidad al derecho a la autodeterminación informativa.- III.- ENFOQUE REGIONAL. Encuadramiento en la realidad comparada del Mercosur.- IV.- ENFOQUE GENÉTICO. Antecedentes de la ley nueva ley.- V.- ENFOQUE CONTEXTUAL. Encuadramiento en el marco normativo preexistente, de nivel constitucional, legislativo y reglamentario.- VI.- ENFOQUE TEXTUAL. Análisis de la ley a través de tres aspectos principales: el régimen de protección de datos personales de carácter comercial, su garantía jurisdiccional, y su control administrativo.- VII.- CONCLUSIÓN. El desafío de construir.

I. INTRODUCCIÓN

Con fecha 1º de octubre de 2004 se publicó en el Diario Oficial de la República Oriental del Uruguay la ley Nº 17.838 de 24 de setiembre de 2004, día de su promulgación por el Poder Ejecutivo.

En virtud de la misma, en lo sustancial, se regula la protección de datos personales de carácter comercial, se estatuye una acción jurisdiccional especial para la protección de todo tipo de datos personales, y se crea un órgano administrativo de control del tratamiento de los datos personales de carácter comercial.

El abordaje de dicho acto legislativo en el marco del ordenamiento positivo nacional relativo al tratamiento jurídico de los datos personales, sugiere la conveniencia de analizarlo desde un quíntuple enfoque: conceptual, regional, genético, contextual y textual.

II. Enfoque Conceptual

En reiteradas oportunidades anteriores,[1] con base en sólida constatación[2], he señalado que «Todo ser humano guarda siempre un misterio en su corazón, una zona reservada a la mirada indiscreta de cualquier otro, que constituye el núcleo más hondo y arraigado de su personalidad, aquello que le hace sentirse autónomo y diferente. Se trata de todo ese mundo interior donde anidan y se esconden los sentimientos, deseos, ilusiones, pensamientos, alegrías y penas, nostalgias o vergüenzas, experiencias e historias, acontecimientos y omisiones..., que son nuestro patrimonio más auténtico, lo único que nos pertenece por completo, porque nos hace sentirnos como sujetos personales, no como un objeto cualquiera expuesto a la contemplación curiosa de los demás».

El reconocimiento explícito de este derecho es relativamente reciente y reconoce una evolución que puede examinarse a través de ciclos sucesivos, sentidos diferentes y enfoques diversos, en cuyo marco procede ubicar el tratamiento actual de los datos personales.

En cuanto a la evolución histórica del derecho a la intimidad, es habitual señalar como hito fundamental en su perfilamiento, el clásico «right to be alone» (1890), es decir, el derecho a ser dejado solo o a ser dejado en paz o a no ser importunado. Este concepto de «privacy» apuntó básicamente a una protección jurídica contra la publicidad de actos o datos personales puestos en conocimiento del público sin noticia o permiso de la persona afectada. Posteriormente, dicho concepto se extendió para abarcar el derecho de los individuos, grupos o instituciones para determinar por sí mismos cuándo, cómo y con qué extensión puede ser comunicada a terceros la información acerca de aquéllos.

En cuanto al sentido de este derecho, el mismo ha transitado desde un sentido negativo (meramente garantista) hacia un sentido positivo. Al respecto, se ha señalado que hasta la consolidación de la sociedad industrial, el «right to privacy» constreñía su contenido al conjunto de facultades de exclusión de ingerencias de terceros en la esfera íntima. En cambio, a partir de la segunda mitad del siglo XX comienza a adquirir un sentido positivo, en la medida que ya no sólo se trata de establecer barreras para preservar la integridad de la dimensión interior del individuo sino que además se afirma la «privacy» como un presupuesto del ejercicio de otros derechos con proyección social e incluso económica.

En cuanto al modo de encarar la protección de la intimidad, se advierte que originalmente el diseño de su tutela se fundó en el concepto de propiedad, extendiendo como medios de protección las herramientas jurídicas pensadas para la tutela del dominio. Ello ha permitido hablar de una visión «patrimonialista» de Derecho privado, luego superada por un enfoque desde la perspectiva del Derecho público que pone el acento en la eminente dignidad humana y en la protección de sus derechos fundamentales.

1 Delpiazzo, Carlos E. *"Dignidad humana y Derecho"*, U.M., Montevideo, 2001, pp. 123 y ss.; *"Protección de los datos personales en tiempos de Internet. El nuevo rostro del derecho a la intimidad"*, en Rev. de Derecho de la Universidad Católica del Uruguay, Montevideo, 2002, Nº III, pp. 253 y ss.; y *"El derecho a la intimidad en el ciberespacio"*, en Anales de las 30 Jornadas Argentinas de Informática e Investigación Operativa, Buenos Aires, 2001, pp. 51 y ss.

2 López Azpitarte, Eduardo. *"Ética y vida"*, Edic. Paulinas, Madrid, 1990, p. 330.

La irrupción de la Informática primero[3] y de la Telemática después, como resultante de su encuentro con las Telecomunicaciones,[4] ha replanteado la cuestión del derecho a la intimidad en atención al riesgo que para la persona implica la estructuración de grandes bancos de datos de carácter personal, y particularmente, la potencialidad del entrecruzamiento de información contenida en ellos.

A partir de esa realidad, *«la libertad informática»*[5] aparece como un nuevo derecho de autotutela de la propia identidad informática, o sea, el derecho de controlar (conocer, corregir, quitar o agregar) los datos personales inscritos en un programa electrónico.

Frente al «poder informático» de quienes pueden acumular informaciones sobre cada persona en cantidad ilimitada, de memorizarla, usarla y transferirla como una mercancía, el derecho a la intimidad se configura como una nueva forma de libertad personal, ya no caracterizada negativamente como la posibilidad de refutar o evitar el uso de datos referidos a cada uno, sino positivamente como la potestad de ejercer un poder de control sobre las informaciones referidas a la propia persona. Consiste en lo que ha dado en llamarse libertad informática, consistente en el derecho de autotutela de la propia identidad informática, es decir, en el derecho de vigilar los datos personales incluidos en archivos automatizados.

Frente a las posibilidades tecnológicas de conseguir un «ciudadano de cristal», la libertad informática es el derecho de disponer de la información personal, de preservar la propia identidad informática o, lo que es lo mismo, de consentir, controlar y rectificar los datos informativos concernientes a la propia personalidad; al derecho de informar y de ser informado se ha agregado el derecho de proteger la libertad de la información como un bien personal, que constituye un nuevo derecho fundamental, propio de la tercera generación, que tiene por finalidad el control que a cada uno de nosotros nos corresponde sobre la información que nos concierne personalmente.

Teniendo en cuenta esta realidad, la doctrina y jurisprudencia alemanas han preferido hablar del *«derecho a la autodeterminación informativa»*[6] a partir del sonado caso resuelto por el Tribunal Constitucional en la sentencia de 15 de diciembre de 1983, en la cual se examinó la constitucionalidad de la ley de censo de población, concluyéndose que no sería compatible con el derecho a la autodeterminación informativa un orden social y un orden jurídico que

3 Delpiazzo, Carlos E. *"Información, Informática y Derecho"*, A.M.F., Montevideo, 1989, pp. 67 y ss.

4 Delpiazzo, Carlos E. *"Derecho de la Informática y las Telecomunicaciones"* (separata del XXIX Curso de Derecho Internacional, Washington, 2002), pp. 395 y ss.; *«El Derecho telemático: respuesta a la convergencia tecnológica»*, en VII Congreso Iberoamericano de Derecho e Informática, Lima, 2000, pp. 54 y ss.; *«El Derecho ante las telecomunicaciones, la informática e Internet»*, en anuario Derecho Informático, F.C.U., Montevideo, 2003, t. III, pp. 41 y ss.; y Delpiazzo, Carlos E. y Viega, María José - *"Lecciones de Derecho Telemático"*, F.C.U., Montevideo, 2004, pp. 73 y ss.

5 Delpiazzo, Carlos E. *"Poder y libertad informática"*, en Rev. Sistemas de Informática, Montevideo, 1985, pp. 16 y 17; y *"Nuevamente sobre poder y libertad informáticos"*, en Primeras Jornadas Nacionales de Derecho Informático, Montevideo, 1987, pp. 147 y ss.

6 Denninger, Erhard *"El derecho a la autodeterminación informativa"*, en A.A.V.V. «Problemas actuales de la documentación y la informática jurídica», Tecnos, Madrid, 1987, pp. 268 y ss.; Hassemer, Winfried y Chirino Sánchez, Alfredo *"El derecho a la autodeterminación informativa y los retos del procesamiento automatizado de datos personales"*, Edit. del Puerto, Buenos Aires, 1997, pp. 166 y ss.; y Murillo De La Cueva, Pablo Lucas *"El derecho a la autodeterminación informativa"*, Tecnos, Madrid, 1990.

hiciesen posible «el que el ciudadano ya no pudiera saber quién, qué, cuándo y con qué motivo se sabe algo sobre él... La libre eclosión de la personalidad presupone en las condiciones modernas de la elaboración de datos la protección del individuo contra la recogida, el almacenamiento, la utilización y la transmisión ilimitadas de los datos concernientes a su persona».

Finalmente, cabe destacar que un sector de la doctrina utiliza la expresión «*derecho a la protección de datos personales*»[7] para designar el derecho bajo examen cuyo objeto es la protección de una parte sustancial del derecho a la intimidad: la que se refiere a la información individual.

Es que hoy resulta extraordinariamente sencillo acceder a datos personales como el nombre, apellidos, domicilio, teléfono, fax, dirección de correo electrónico o estado civil que, pudiendo parecer inocuos, al cruzarlos con los hábitos de consumo o al tratarlos con programas *datamining* -dedicados a buscar información sensible escondida dentro de bases de datos- nos proporcionan, al entrecruzarse como haces de luz, una silueta virtual perfecta que refleja el yo más íntimo del potencial consumidor, perfecta representación de sus tendencias naturales, intuitivas e instintivas.

Muchas veces, los datos personales son facilitados voluntariamente por el propio titular de los mismos para acceder gratuitamente a algún servicio o para la obtención onerosa de un bien a través de Internet sin tener conciencia de que los mismos pueden ser utilizados para fines diferentes de aquellos para los que fueron recabados. Pero otras veces los datos del internauta son dejados por éste de manera completamente involuntaria ya que, una vez que los mismos salen de su computador, desconoce la ruta que siguen hacia su destino, en qué puntos intermedios se almacenan temporalmente y quién puede acceder a ellos, copiarlos, modificarlos y utilizarlos para cualquier finalidad diferente de aquélla para la que fueron entregados.

Por eso, sin perjuicio de los textos positivos expresos que se han ido aprobando, es necesario reivindicar la importancia y plena vigencia en el ciberespacio de los principios generales de Derecho como sólidos soportes de tutela efectiva de todos los derechos fundamentales, incluidos los de novísima generación, como el que nos ocupa.[8]

III. Enfoque Regional

Nuestro país se encuentra inmerso en el proceso de integración regional denominado Mercado Común del Sur (Mercosur), conformado conjuntamente con Argentina, Brasil y

7 Ekmekdjian, Miguel Angel y Pizzolo, Calogero, *"Habeas data. El derecho a la intimidad frente a la revolución informática"*, Depalma, Buenos Aires, 1996, pp. 5 y ss.; Telez Valdés, Julio, *"Derecho Informático"*, Mc Graw Hill, México, 2004, 3ª ed., pp. 57 y ss.; Davara Rodríguez, Miguel Angel, *"Manual de Derecho Informático"*, Thomson - Aranzadi, Navarra, 2004, 6ª edición, pp. 43 y ss.; Ortega Giménez, Alfonso, *"El derecho a la protección de datos de carácter personal en Internet"*, en X Congreso Iberoamericano de Derecho e Informática, Santiago de Chile, 2004, pp. 223 y ss.; y Canales Gil, Alvaro, *"La protección de datos personales como derecho fundamental"*, en anuario "Derecho Informático", F.C.U., Montevideo, 2004, t. IV, pp. 261 y ss.

8 Delpiazzo, Carlos E. *"Regulación de Internet"*, en anuario "Derecho Informático", F.C.U., Montevideo, 2001, t. I, pp. 71 y ss.; y *"¿Hacia dónde va el Derecho de Internet?"*, en anuario "Derecho Informático", F.C.U., Montevideo, 2004, t. IV, pp. 255 y ss.

Paraguay.[9] A diferencia de los demás, Uruguay es el único país cuya Constitución carece de norma explícita en materia de protección de datos personales, sin perjuicio de construcciones teóricas acerca de su reconocimiento implícito en el art. 72, según se expondrá más adelante.

En cambio, en **Argentina**, sin perjuicio de valiosos antecedentes en las Constituciones provinciales, la Constitución nacional reformada en 1994 prevé el habeas data en su art. 43, inc. 3º, a cuyo tenor toda persona podrá interponer acción «para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos».[10]

Desarrollando el precepto, se dictó la ley Nº 25.326 de 30 de octubre de 2000,[11] en la cual se desarrolla en 7 capítulos y está compuesta por 48 artículos:

a) en el capítulo I se establece su objeto como «la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos o privados, destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre» (art. 1º), y se incorporan un conjunto de definiciones (art. 2º);
b) el capítulo II está dedicado a los principios generales relativos a la protección de datos, consagrando los de licitud (art. 3º), calidad de los datos (art. 4º), consentimiento (art. 5º), confidencialidad (art. 10) y otros relativos a determinados datos, tales como los de salud (art. 8º);
c) el capítulo III trata de los derechos de los titulares de datos, enfatizando en los de información (art. 13) y acceso (art. 14 y sigtes.);
d) el capítulo IV se refiere a los usuarios y responsables de archivos, registros y bancos de datos, imponiendo la registración en el órgano de control (art. 21 y sigtes.);
e) en el capítulo V se regulan las facultades de dicho órgano de control (arts. 29 y 30);
f) el capítulo VI está dedicado a las sanciones administrativas y penales aplicables (arts. 31 y 32); y
g) en el capítulo VII se normatiza acerca de la acción de protección de los datos personales o habeas data (art. 33 y sigtes.).

En virtud de esta ley, Argentina es el único país de la región al cual la Comisión de la Unión Europea, por decisión de 20 de junio de 2003, ha reconocido que «garantiza un nivel adecuado de protección por lo que respecta a los datos personales transferidos desde la Comunidad» (art. 1º).

9 Gros Espiell, Héctor; Delpiazzo, Carlos E.; Rotondo, Felipe; Vázquez, Cristina; y Brito, Mariano. *"El Derecho de la Integración del Mercosur"*, U.M., Montevideo, 1999.

10 Dromi, Roberto, y Menem, Eduardo, *"La Constitución Reformada"*, E.C.A., Buenos Aires, 1994, pp. 167 y ss.

11 Gozaini, Osvaldo Alfredo (Coordinador), *"La defensa de la intimidad y de los datos personales a través del habeas data"*, Ediar, Buenos Aires, 2001.

En **Brasil**, el art. 5º, inc. LXXII de la Constitución Federal de 1988 preceptúa que «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».

En virtud de la ley Nº 9.507 de 12 de noviembre de 1997, que consta de 23 artículos, se regula el derecho de acceso a informaciones de carácter personal y se disciplina el proceso de habeas data[12]:

a) por el art. 1º se considera de carácter público todo registro o banco de datos que contenga informaciones que sean o puedan ser trasmitidas a terceros o que no sean de uso privativo del órgano o entidad productora o depositaria de informaciones, regulándose con plazos la obligación de brindar información a los requirentes (art. 2º y sigtes.); y
b) a partir del art. 7º se regula la acción de habeas data en sus aspectos sustantivos y procesales.

En **Paraguay**, el art. 33 de la Constitución de 1992 reconoce que "La intimidad personal y familiar, así como el respeto a la vida privada, son inviolables", agregando que "Se garantizan el derecho a la protección de la intimidad, de la dignidad y de la imagen privada de las personas".

A su vez, el art. 135 se refiere al habeas data en los siguientes términos: "Toda persona puede acceder a la información y a los datos que sobre sí misma, o sobre sus bienes, obren en registros oficiales o privados de carácter público, así como conocer el uso que se haga de los mismos y de su finalidad. Podrá solicitar ante el magistrado competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectaran ilegítimamente sus derechos".

Desarrollando la normativa constitucional, la ley Nº 1.682 de 16 de enero de 2001, modificada parcialmente por la ley Nº 1.969 de 2 de setiembre de 2002, tiene por objeto "regular la recolección, almacenamiento, distribución, publicación, modificación, destrucción, duración y, en general, el tratamiento de datos personales contenidos en archivos, registros, bancos de datos o cualquier otro medio técnico de tratamiento de datos públicos o privados, destinados a dar informes, con el fin de garantizar el pleno ejercicio de los derechos de sus titulares".

IV. Enfoque Genético

Sin perjuicio de otros antecedentes,[13] el texto de la ley Nº 17.838 encuentra su origen en el **proyecto de ley presentado el 6 de mayo de 2003** por los Senadores Alberto Brause y Luis Alberto Heber, en la Cámara Alta del Poder Legislativo, bajo el título "Protección de datos personales para informes comerciales".[14]

12 Alvim Wambier, Teresa Arruda, *"Habeas data"*, Edit. Revista dos Tribunais, Sao Paulo, 1998.

13 Delpiano, Héctor Miguel, *"Protección de datos personales. Bancos de datos de información crediticia"*, F.C.U., Montevideo, 1997, pp. 25 y ss.

14 Ver: texto del proyecto en anuario "Derecho Informático", F.C.U., Montevideo, 2004), t. IV, pp. 421 y ss.

Dicha iniciativa constaba de 24 artículos agrupados en 7 capítulos, a saber:

a) "Disposiciones generales" relativas al ámbito de aplicación (arts. 1º y 2º);
b) "Principios generales" que informan el tratamiento de datos personales con finalidad comercial (arts. 3º a 7º);
c) "De los derechos de los titulares de datos", con especial referencia al ejercicio del derecho de acceso (arts. 8º a 11);
d) "Del tratamiento de datos personales relativos a obligaciones de carácter comercial" (arts. 12 a 15);
e) "Acción de protección de los datos personales o habeas data" (arts. 16 a 18);
f) "Órgano de control" (arts. 19 y 20); y
g) "Disposiciones finales y transitorias" tendientes a la puesta en práctica del régimen propuesto (arts. 21 a 24).

A juicio del Instituto de Derecho Informático de la Facultad de Derecho de la Universidad de la República, en **dictamen de 6 de agosto de 2003**,[15] la iniciativa mereció la calificación de valiosa en cuanto recogía soluciones y principios avanzados en materia de protección de la autodeterminación informativa de las personas.

No obstante, se destacó como cuestión a revisar el que la limitación de su objeto proyectaba un acotamiento lamentable sobre el alcance del habeas data, que debería extenderse a la protección de todo dato personal (y no sólo los de carácter comercial).

Asimismo, se entendió que debería reexaminarse la configuración del órgano de control, el cual debe estar dotado de un estatuto jurídico que garantice su autonomía técnica.

Acogiendo parcialmente tales recomendaciones, la Comisión de Constitución y Legislación de la Cámara de Senadores revisó el proyecto con la doble finalidad de mantener el objetivo inicial de regular el tratamiento de los datos personales de carácter comercial y dar mayor alcance a la acción de habeas data, abarcando la protección de cualquier dato personal. Consecuentemente, se elaboró un **proyecto sustitutivo fechado el 13 de abril de 2004**,[16] el cual se estructuró en tres partes, a saber:

a) un Título I, innominado, comprensivo de tres capítulos:

- Capítulo I, "Protección de datos personales de informes comerciales" (arts. 1º y 2º),
- Capítulo II, "Principios generales" (arts. 3º a 7º), y
- Capítulo III, "Del tratamiento de datos personales relativos a obligaciones de carácter comercial" (arts. 8º a 11);

15 Ver: dictamen del Instituto de Derecho Informático de 6 de agosto de 2003 en anuario "Derecho Informático", F.C.U., Montevideo, 2004, t. IV, pp. 427 y ss.

16 Ver: texto en Diario de Sesiones de la Cámara de Senadores correspondiente al 8 de junio de 2003.

b) un Título II, relativo a "Habeas data y Órgano de control", abarcativo de otros tres capítulos:

- Capítulo I, "Habeas data" (arts. 12 a 16),
- Capítulo II, "Acción de protección de datos personales" (arts. 17 a 19), y
- Capítulo III, "Órgano de control" (arts. 20 y 21); y

c) un Título III, referente a "Disposiciones finales y transitorias" (arts. 22 a 26).

Con leves modificaciones, **la Cámara de Senadores dio aprobación al proyecto con fecha 8 de junio de 2004**,[17] el que, consecuentemente, pasó a la Cámara de Representantes.

En esta nueva instancia, el Instituto de Derecho Informático emitió **su dictamen de 28 de julio de 2004**,[18] en el cual, tras reseñar los antecedentes del caso y analizar el proyecto de ley aprobado por el Senado, se constató que mientras que el proyecto original tenía por único objeto la regulación de los datos personales de carácter comercial, el aprobado realiza un importante distingo, en la línea sugerida por el Instituto de Derecho Informático en su dictamen ya referido.

En efecto, en tanto que su Título I mantiene la limitación de su objeto a los "datos personales asentados en archivos, registros, bases de datos u otros medios de tratamiento de los mismos, sean éstos públicos o privados, destinados a brindar informes objetivos de carácter comercial" (art. 1º), su Título II regula con alcance general la acción de habeas data, reconociendo ampliamente que "Toda persona tendrá derecho a entablar una acción efectiva para tomar conocimiento de los datos referidos a su persona y de su finalidad y uso, que consten en bancos de datos públicos o privados y, en caso de error, falsedad o discriminación, a exigir su rectificación, supresión o lo que entienda corresponder" (art. 12).

No obstante tal aspecto positivo, se señaló la preocupación subsistente por el "déficit que registra la iniciativa al no contemplar un órgano de control dotado de autonomía técnica... en tanto no se ha optado por ninguna de las soluciones generalmente aceptadas por el Derecho comparado ni se han tenido en cuenta las fórmulas organizativas usadas en nuestro país en materia de órganos reguladores y de control".

Lamentablemente, quizás debido a la premura impuesta a la labor legislativa por la finalización del período de sesiones, **la Cámara de Representantes dio aprobación al proyecto el 8 de setiembre de 2004**, tal como venía del Senado, por lo que el **texto promulgado por el Poder Ejecutivo el 24 de setiembre de 2004** es el resultante de la versión trabajada por la Cámara de Senadores.[19]

17 Ver: debate y texto aprobado en Diario de Sesiones de la Cámara de Senadores correspondiente al 8 de junio de 2003, pp. 269 y ss., y 275 y ss.

18 Ver: dictamen del Instituto de Derecho Informático de 28 de julio de 2004 en anuario "Derecho Informático", F.C.U., Montevideo, 2005, t. V.

19 Ver: Diario Oficial Nº 26.599 de 1º de octubre de 2004, pp. 4-A y ss.

V. Enfoque Contextual

La sanción de la iniciativa cuya génesis viene de reseñarse sintéticamente, se inscribe en un contexto normativo de cuya consideración no puede prescindirse para la cabal interpretación de la ley Nº 17.838.[20]

A nivel constitucional, si bien nuestra Carta Política no consagra expresamente el derecho a la protección de los datos personales -a diferencia de lo que acontece en otros textos constitucionales de la región- el mismo debe considerarse reconocido al máximo nivel normativo en base al **art. 72** de la Carta, a cuyo tenor «La enumeración de derechos, deberes y garantías hecha por la Constitución, no excluye los otros que son inherentes a la personalidad humana o se derivan de la forma republicana de gobierno».

Por eso, antes de ahora, he opinado que la libertad informática y su garantía, que es el habeas data, se encuentran reconocidos en dicho art. 72,[21] en la medida que éste incorpora al ordenamiento jurídico positivo nacional la esencia ideológica del jusnaturalismo[22] y, consecuentemente, tutela efectivamente los derechos del hombre inherentes a su personalidad, garantizándolos.[23] Asimismo, tal acogimiento de dicha estimativa jusnaturalista encarta en la Constitución a los principios generales de Derecho que son derivación de la eminente dignidad humana que ella reconoce expresamente.

Más específicamente, el **art. 28** prevé que "Los papeles de los particulares y su correspondencia epistolar, telegráfica o de cualquier otra especie, son inviolables, y nunca podrá hacerse su registro, examen o interceptación sino conforme a las leyes que se establecieren por razones de interés general".

A partir de dicha disposición, particularmente con referencia a las comunicaciones telefónicas, se ha postulado que "la norma constitucional garantiza no sólo la inviolabilidad del contenido de las conversaciones telefónicas sino también -como consecuencia de la prohibición de su registro- la inviolabilidad de toda lista o nómina de las llamadas que se han hecho, de qué llamadas se han recibido, y de entre quiénes y cuándo... La inviolabilidad cubre no sólo el contenido sino la existencia misma de las comunicaciones telefónicas y, por ende, su difusión y conocimiento por terceros".[24]

20 Delpiazzo, Carlos E. *"Estado de la protección de datos personales en Uruguay"*, en anuario "Derecho Informático", F.C.U., Montevideo, 2004, t. IV, pp. 271 y ss.

21 Delpiazzo, Carlos E. *"Posibles medios de protección frente a las responsabilidades derivadas de la gestión de bases de datos en el Derecho uruguayo"*, en Congreso Internacional de Informática y Derecho, Buenos Aires, 1990, pp. 382 y ss.

22 Real, Alberto Ramón, *"Estado de Derecho y humanismo personalista"*, F.C.U., Montevideo, 1974, pp. 5 y ss.

23 Gros Espiell, Héctor, *"La dignidad humana en los instrumentos internacionales de derechos humanos"*, en Cátedra UNESCO de Derechos Humanos, *"Dignidad Humana"* (Universidad de la República, Montevideo, 2003), pp. 9 y ss.; y Cagnoni, José Aníbal, *"La dignidad humana. Naturaleza y alcances"*, en Cátedra UNESCO de Derechos Humanos, *"Dignidad Humana"* cit., pp. 65 y ss., y en Rev. de Derecho Público, Año 2003, Nº 23, pp. 11 y ss.

24 Gros Espiell, Héctor. *"El art. 28 de la Constitución y las comunicaciones telefónicas"*, en Rev. de Administración Pública, Montevideo, 1999, Nº 25, p. 86.

Además, en la medida que la tutela de los datos personales puede considerarse una prolongación del derecho a la intimidad, consistente en que no se produzca ningún tipo de intromisiones en el ámbito reservado a la vida privada de los individuos, cabe hacer caudal también del **art. 10**, cuyo inc. 1º dispone que «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».[25]

A nivel legislativo, cabe tener presente, en primer lugar, que el **Pacto Internacional de Derecho Civiles y Políticos,**[26] en línea con otros instrumentos internacionales, prevé en su art. 17 que «Nadie será objeto de ingerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación».

En segundo lugar, el **Pacto de San José de Costa de Rica** reconoce en su art. 11, num. 2, que «Nadie puede ser objeto de ingerencias 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».[27]

En tercer lugar, cabe hacer caudal de la **normativa reguladora del secreto**, tanto en materia de identificación civil (de acuerdo al art. 21 del decreto ley Nº 14.762 de 13 de febrero de 1978) como tributaria (según lo previsto en el Código Tributario aprobado por decreto ley Nº 14.306 de 29 de noviembre de 1974) y bancaria (conforme a lo dispuesto en el decreto ley de intermediación financiera Nº 15.322 de 17 de setiembre de 1982).

En cuarto lugar, la **ley Nº 16.616 de 20 de octubre de 1994**, regulatoria del Sistema Estadístico Nacional, incluye disposiciones que, no obstante estar referidas a los datos estadísticos, tienen importancia en la medida que explicitan para tal caso principios generales relativos al tratamiento de los datos.[28]

Así, de acuerdo a su art. 3, «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».

A continuación, el mismo art. 3 define cada uno de dichos principios, correspondiendo destacar especialmente los siguientes:

a) «El secreto estadístico obliga a tratar los datos individuales proporcionados por la fuente de información con la más absoluta confidencialidad, de forma tal de no revelar la identificación de dichas fuentes».

[25] KORZENIAK, José. *"Curso de Derecho Constitucional 2º"*, F.C.U., Montevideo, 1971, vol. 1, pp. 147 y 148; y RISSO FERRAND, Martín J. *"Derecho Constitucional"*, Ingranusi, Montevideo, 1998, t. III, pp. 131 y 132.

[26] Ratificado en virtud de la ley Nº 13.751 de 11 de julio de 1969.

[27] Ratificado en virtud de la ley Nº 15.737 de 8 de marzo de 1985.

[28] DELPIAZZO, Carlos E. *"Derecho Informático Uruguayo"*, Idea, Montevideo, 1995, pp. 177 y ss.

b) «La pertinencia es el vínculo que debe existir entre los datos solicitados a la fuente de información y los objetivos de la actividad estadística para la cual dichos datos son recabados».
c) «La transparencia es el derecho de las fuentes de información de conocer los objetivos de la actividad estadística para la cual se solicitan los datos, y si los mismos estarán amparados por el secreto estadístico».
d) «La rigurosidad consiste en la aplicación sistemática de los principios, métodos y procedimientos generalmente aceptados por la técnica y la ciencia estadística».

A su vez, el art. 16 de la misma ley Nº 16.616 refiere al principio de finalidad en los siguientes términos: «Los datos individuales aportados con fines estadísticos no pueden ser utilizados con otros fines, ni aun mediando solicitud expresa del informante».

En quinto lugar, es preciso citar el **art. 694 de la ley Nº 16.736 de 5 de enero de 1996**, a cuyo tenor «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». La referencia al «pleno acceso a las informaciones de su interés» implica el reconocimiento de la libertad informática y conlleva los derechos inherentes a la misma de obtener la rectificación o eliminación según corresponda, del dato erróneo, falso o inexacto.[29]

En sexto lugar, cabe mencionar la **ley Nº 17.823 de 7 de setiembre de 2004**, por la que se aprobó el Código de la Niñez y la Adolescencia, normatizando expresamente en materia de datos personales de los menores. Conforme a su art. 218, se establece que "El Instituto Nacional del Menor deberá desarrollar el Sistema Nacional de Información sobre Niñez y Adolescencia, que deberá incluir datos sobre el niño o adolescente a su cargo y las instituciones que lo atienden". Agrega el art. 219 que "El Sistema Nacional de Información sobre Niñez y Adolescencia deberá generar datos que permitan un adecuado seguimiento de la atención del niño o adolescente y de la evolución de la misma, así como generar la información necesaria para la formulación de las políticas de niñez y adolescencia".

De acuerdo al art. 221, "El Instituto Nacional del Menor será el custodio de la información contenida en el Sistema Nacional de Información sobre Niñez y Adolescencia, por lo que 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 personal, como único propietario de la misma".

Consecuentemente, "La información relativa a niños y adolescentes no podrá ser utilizada como base de datos para el rastreo de los mismos, una vez alcanzada la mayoría de edad"

[29] DELPIAZZO, Carlos E. *"Automatización de la actividad administrativa en el marco de la reforma del Estado"*, en Anuario de Derecho Administrativo, Montevideo, 1998, t. VI, pp. 17 y ss.; *«El procedimiento administrativo electrónico y el acto administrativo automático»*, en A.A.V.V. *"Recopilación de conferencias y exposiciones realizadas"*, UTE, Montevideo, 1999, pp. 39 y ss.; *«Marco legal de la automatización de la actividad administrativa. El expediente electrónico en Uruguay»*, en Informática y Derecho, Mérida, 1998, Nº 19 - 22, pp. 699 y ss.; y *«Enfoque jurídico de la automatización de la actividad administrativa»*, en Rev. Informática y Derecho, Buenos Aires, 2002, vol. 8, pp. 81 y ss.

y "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" (art. 222).

En séptimo lugar, en lo que puede considerarse una limitante justificada a la normativa reguladora del secreto, la **ley Nº 17.835 de 23 de setiembre de 2004** impone que "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".

A nivel reglamentario, cabe hacer referencia en primer lugar al **Decreto Nº 258/992 de 16 de junio de 1992**, cuyo art. 17 dispuso que "El médico debe llevar un registro escrito de todos los procedimientos, sean diagnósticos o terapéuticos, que indique al paciente, estando obligado a consignar la semiología realizada y la evolución del caso. Dicho registro, llevado en ficha o historia clínica, sea en forma escrita, electrónica u otra, constituirá, de por sí, documentación auténtica y hará plena fe de su contenido a todos sus efectos".[30]

A su vez, el art. 40 reconoció que "El paciente tiene derecho a que se respete su intimidad mientras permanezca en el hospital y se trate confidencialmente toda la información y los documentos relativos al estado de su salud". Agrega el art. 41 que "El paciente tiene derecho a revisar su historia clínica y a obtener una copia de la misma a sus expensas".

Sin perjuicio de dicho antecedente, la norma clave en materia de datos de salud la constituye actualmente el **Decreto Nº 396/003 de 30 de setiembre de 2003**, que trata de los datos personales relativos a la salud.[31]

En virtud de su art. 8º, que encabeza el capítulo II, titulado "Principios y objetivos", se establece que "El sistema de historia clínica electrónica única de cada persona, deberá ajustarse en todo momento a los siguientes principios generales:

a) finalidad;
b) veracidad;
c) confidencialidad;
d) accesibilidad; y
e) titularidad particular.

[30] DELPIAZZO, Carlos E. *"¿Es legal la historia clínica electrónica?"*, conferencia pronunciada en el Salón de Actos del Sindicato Médico del Uruguay el 19 de agosto de 1999; y *"La historia clínica electrónica"*, en El Derecho Digital (www.elderechodigital.com.uy).

[31] DELPIAZZO, Carlos E. *"Acerca del Decreto Nº 396/003 de 30 de setiembre de 2003 sobre Historia Clínica Electrónica"*, en Boletín Informativo de la Sociedad Uruguaya de Informática en Salud, Montevideo, 2003, Nº 17, pp. 3 y ss.; y *"Historia clínica electrónica. A propósito de su marco regulatorio en Uruguay"*, en X Congreso Iberoamericano de Derecho e Informática, Santiago de Chile, setiembre de 2004, pp. 237 y ss.

Dichos principios generales servirán también de criterio interpretativo para resolver las cuestiones que puedan suscitarse en la aplicación de las disposiciones pertinentes".

A continuación, las disposiciones siguientes definen el alcance de cada uno de los referidos principios.

Conforme al art. 9º, se reconoce que, "De acuerdo al *principio de finalidad*, los datos consignados en la historia clínica no podrán ser usados en forma nominada para otros fines que no sean los asistenciales... a menos que medie para ello expreso consentimiento informado del interesado".[32]

Al tenor del art. 10, "El *principio de veracidad* impone incluir en la historia clínica electrónica todos los procedimientos, sean diagnósticos o terapéuticos, que se indiquen al paciente" en forma inteligible para éste y que no pueda ser alterada.[33]

De acuerdo al art. 11, "El *principio de confidencialidad* obliga a tratar los datos relativos a la salud de la persona con la más absoluta reserva. A tal efecto, la historia clínica electrónica deberá contar con una estructuración que separe la información de identificación del titular del resto de los datos consignados, pudiendo asociarse ambas únicamente en el ámbito de la atención médica del titular de la historia clínica".[34]

"En aplicación del *principio de accesibilidad* -reza el art. 13- el titular de los datos tendrá en todo momento derecho a conocerlos, a que le sean explicados y a que se rectifiquen si fueran probadamente erróneos".[35]

Finalmente, el art. 15 reconoce el *principio de titularidad* al establecer que "Siendo los datos contenidos en la historia clínica electrónica de titularidad de la persona a que refieren, sólo ésta o sus derechohabientes podrán autorizar el uso por terceros de la información total o parcial en ella contenida".[36]

VI. Enfoque Textual

Según se señaló al principio, tres aspectos principales constituyen el contenido esencial de la ley Nº 17.838, a saber:

a) el régimen de protección de los datos personales de informes comerciales;
b) la llamada acción jurisdiccional de habeas data; y

[32] DELPIAZZO, Carlos E. *"Protección de los datos personales en tiempos de Internet. El nuevo rostro del derecho a la intimidad"*, cit., pp. 253 y ss.

[33] DELPIAZZO, Carlos E. *"Normas y principios de la contratación administrativa"*, F.C.U., Montevideo, 2002, pp. 32 y ss.

[34] DELPIAZZO, Carlos E. *"Dignidad humana y Derecho"* cit., pp. 135 y ss.

[35] SÁNCHEZ CARNELLI, Lorenzo. *"Honor, dignidad del individuo, bases de datos y habeas data"*, en Rev. de Derecho Público (Montevideo, 2004), Nº 25, pp. 73 y ss.

[36] DELPIAZZO, Carlos E. y VIEGA, María José. *"Lecciones de Derecho Telemático"* cit., pp. 224 y ss.

c) el control administrativo del tratamiento de los datos personales de carácter comercial, tanto en el ámbito público como privado.

Con relación al primero de los temas indicados, la ley comienza distinguiendo entre los datos personales "destinados a brindar informes objetivos de carácter comercial" a los que se dirige su regulación (art. 1º, inc. 1º) y los demás datos de carácter personal, sea que ellos se originen en el ejercicio de libertades o que sean de los llamados sensibles, "entendiéndose por éstos aquellos datos referentes al origen racial y étnico de las personas, así como sus preferencias políticas, convicciones religiosas, filosóficas o morales, afiliación sindical o información referente a su salud física o a su sexualidad y toda otra zona reservada a la libertad individual" (art. 2º, inc. 1º).

Mientras que "Para la obtención y tratamiento de datos que no sean de carácter comercial se requerirá expresa y previa conformidad de los titulares, luego de informados del fin y alcance del registro en cuestión" (art. 2º, inc. 2º), "No requiere previo consentimiento el registro y posterior tratamiento de datos personales cuando (arts. 4º y 8º):

a) Los datos provengan de fuentes públicas de información, tales como registros, archivos o publicaciones en medios masivos de comunicación;
b) Sean recabados para el ejercicio de funciones o cometidos constitucional y legalmente regulados propios de las instituciones del Estado o en virtud de una obligación específica legal;
c) Se trate de listados cuyos datos se limiten a nombres y apellidos, documento de identidad o registro único de contribuyente, nacionalidad, estado civil, nombre del cónyuge, régimen patrimonial del matrimonio, fecha de nacimiento, domicilio y teléfono, ocupación o profesión y domicilio;
d) Deriven de una relación contractual del titular de los datos y sean necesarios para su desarrollo y cumplimiento; y
e) Se realice por personas físicas o jurídicas, privadas o públicas, para su uso exclusivo o el de sus asociados o usuarios".

Por lo demás, la nueva ley alcanza al tratamiento de datos comerciales, tanto de personas físicas como jurídicas, involucrando "toda forma de registro, almacenamiento, distribución, transmisión, modificación, eliminación, duración y toda otra forma del mismo o similar alcance" (art. 1º, inc. 2º).

Respecto a dicho tratamiento, en línea con la enseñanza en la materia,[37] se explicitan parcialmente algunos principios generales, tales como:

a) el de legalidad (art. 3º);
b) los principios de veracidad, adecuación, ecuanimidad, proporcionalidad, y lealtad (art. 5º);
c) los de uso reservado y acorde a la finalidad de la colecta (art. 6º); y
d) el de acotamiento temporal a cinco años (art. 9º).

37 DELPIAZZO, Carlos E. y VIEGA, María José. *"Lecciones de Derecho Telemático"* cit., pp. 73 y ss.

Aclara el art. 10 que el tratamiento de la información registrada debe ser "objetivo", es decir, tal cual ésta fuera suministrada, debiendo abstenerse los responsables de bases de datos "de efectuar valoraciones subjetivas sobre la misma".

Con relación a la acción de habeas data, el art. 12 proclama en forma amplia su *alcance*, estableciendo que "Toda persona tendrá derecho a entablar una acción efectiva para tomar conocimiento de los datos referidos a su persona y de su finalidad y uso, que consten en registros o bancos de datos públicos o privados y, en caso de error, falsedad o discriminación, a exigir su rectificación, supresión o lo que entienda corresponder".

Quiere decir que se consagran en forma abarcativa de todo tipo de dato personal, las diversas especies de habeas data que la doctrina ha sistematizado de la siguiente manera[38]:

a) habeas data informativo, que es el que procura lograr el acceso al registro de que se trate, el cual puede ser, a su vez: exhibitorio (cuando se desea conocer qué datos se encuentran registrados), finalista (cuando se pretende indagar para qué y para quién se realizó el registro), y autoral (cuando se persigue el propósito de inquirir acerca de quién obtuvo los datos que obran en el registro);
b) habeas data correctivo, que es el que procura corregir o sanear informaciones falsas, inexactas o imprecisas;
c) habeas data cancelatorio, que es el que procura eliminar la información almacenada cuando ella no debe mantenerse;
d) habeas data aditivo, que es el que procura agregar más datos a los que figuran en el registro de que se trate, sea para actualizar datos vetustos, sea para incluir datos omitidos; y
e) habeas data reservador, que es el que procura asegurar que un dato legítimamente registrado pero de acceso restringido, sea proporcionado solo a quienes corresponda y en las circunstancias que correspondan.

En cuanto a la finalidad del habeas data, es interesante señalar que la ley lo regula como una garantía de acceso a los datos personales (habeas data propio), por oposición a otro tipo de datos no personales, especialmente en poder de administraciones públicas (habeas data impropio). Al respecto, ya he tenido oportunidad de pronunciarme[39] antes de ahora en el sentido de que la segunda de las indicadas hipótesis no es más que una manifestación actual del viejo derecho de acceso de los ciudadanos a los archivos y registros administrativos, cuyo fundamento radica en los principios de publicidad y transparencia de las actuaciones administrativas, el cual resulta reforzado a la luz de recientes normas dictadas para combatir la corrupción.[40]

38 PUCCINELLI, Oscar. *"El habeas data en Indoiberoamérica"*, Temis, Bogotá, 1999, pp. 220 y ss.

39 DELPIAZZO, Carlos E. *"Automatización de la actividad administrativa en el marco de la reforma del Estado»* cit., p. 22.

40 DELPIAZZO, Carlos E. *"De la publicidad a la transparencia en la gestión administrativa"*, en Rev. de Derecho de la Universidad de Montevideo, Montevideo, 2003, Año II, Nº 3, pp. 113 y ss., *"Control social de la Administración y transparencia"*, en Ius Publicum, Santiago de Chile, 2003, Nº 11, pp. 43 y ss.; y *"La regulación legal del control social y transparencia"*, en Rev. de los Antiguos Alumnos del IEEM, Montevideo, 2002, Año 5, Nº 1, pp. 29 y ss.

En cuanto a la *procedencia* de la acción, cabe agregar que la regulación del habeas data se hace en forma subsidiaria del "derecho a obtener toda la información que sobre sí mismo se halle en bases de datos públicas o privadas" directamente ante ellas (arts. 14 a 16). En efecto, el art. 17 dispone que "El titular de datos personales podrá entablar la acción de protección de datos personales o habeas data, contra todo responsable de una base de datos pública o privada, en los siguientes supuestos:

a) cuando quiera conocer sus datos personales que se encuentran registrados en una base de datos o similar y dicha información no le hubiese sido proporcionada por el responsable de la base de datos; o
b) cuando haya solicitado al responsable de la base de datos su rectificación, actualización, eliminación o supresión y éste no hubiese procedido a ello o dado razones suficientes por las que no corresponde lo solicitado, en el plazo previsto al efecto en la ley" (que es de 20 días hábiles desde la solicitud, según lo previsto en el art. 14, inc. 3º).

Respecto a la *legitimación activa*, el art. 18 reconoce que "La acción de habeas data podrá ser ejercida por el propio afectado titular de los datos o sus representantes, ya sean tutores o curadores y, en caso de personas fallecidas, por sus sucesores universales, en línea directa o colateral hasta el segundo grado, por sí o por medio de apoderado. En el caso de las personas jurídicas, la acción deberá ser interpuesta por sus representantes legales o los apoderados designados a tales efectos".

En cuanto a la *tramitación del proceso* originado en el ejercicio de la acción de habeas data, el art. 19 establece que se regirá "en lo general por las normas del Código General del Proceso y en lo particular por los arts. 6º, 7º, 10, 12 y 13 y en lo aplicable por los demás artículos de la ley Nº 16.011 de 19 de diciembre de 1988", que regula la acción de amparo.[41]

De acuerdo a las normas remitidas, resulta que "el Juez convocará a las partes a una audiencia pública dentro del plazo de tres días a partir de la fecha de presentación de la demanda. En dicha audiencia se oirán las explicaciones del demandado, se recibirán las pruebas y se producirán los alegatos... La sentencia se dictará en la audiencia o, a más tardar, dentro de las veinticuatro horas de su celebración" (art. 6º).

"Si de la demanda o en cualquier otro momento del proceso, resultare, a juicio del Juez, la necesidad de su inmediata actuación, éste dispondrá, con carácter provisional, las medidas que correspondieren en amparo del derecho o libertad presuntamente violados" (art. 7º).

"Sólo serán apelables la sentencia definitiva y la que rechaza la acción por ser manifiestamente improcedente. El recurso de apelación deberá interponerse en escrito fundado, dentro del plazo perentorio de tres días. El Juez elevará sin más trámite los autos al superior cuando hubiere desestimado la acción por improcedencia manifiesta y lo sustanciará con un traslado a la contraparte, por tres días perentorios, cuando la sentencia apelada fuese la definitiva. El Tribunal resolverá en acuerdo, dentro de los cuatro días siguientes a la recepción de los autos" (art. 10).

[41] OCHS OLAZABAL, Daniel, *"La acción de amparo"*, F.C.U., Montevideo, 2001, 2ª edición, pp. 29 y ss.; VIERA, Luis Alberto y colaboradoras, *"Ley de amparo"*, Idea, Montevideo, 1993, 2ª edición, pp. 34 y ss.; y BIASCO MARINO, Emilio, *"El amparo general en el Uruguay"*, A.E.U., Montevideo, 1998, pp. 167 y ss.

Además, en la acción de habeas data "no podrán deducirse cuestiones previas, reconvenciones ni incidentes" (art. 12) y "Las normas procesales tendrán el carácter de supletorias en los casos de oscuridad o insuficiencia de las precedentes" (art. 13).

Con relación al control administrativo, prescindiendo de considerar sus bases conceptuales, la ley regula aspectos de organización y de competencia.[42]

Desde el punto de vista de la *organización*, el art. 20, inc. 1º prevé que "El Ministerio de Economía y Finanzas actuará como órgano de control en el tratamiento de datos personales comprendidos en esta ley", o sea, los "destinados a brindar informes objetivos de carácter comercial" (según el art. 1º).

En el desempeño de tal función, actuará "asistido de una Comisión Consultiva integrada por siete miembros, tres de los cuales serán representantes de dicho Ministerio, uno de los cuales la presidirá; dos representantes del Ministerio de Educación y Cultura, un representante de la Cámara Nacional de Comercio y Servicios, y un representante de la Liga de Defensa Comercial" (art. 20, inc. 2º).

Desde el punto de vista de la *competencia*, se faculta al Ministerio de Economía y Finanzas a "aplicar las siguientes medidas sancionatorias a las firmas de tratamiento de datos en caso que se violen las normas de la presente ley" (art. 21):

a) apercibimiento;
b) multa de hasta 200 UR; y
c) clausura del archivo, registro o base de datos respectivo, mediante mandato judicial o administrativamente para el caso de que el Juez no la decretara dentro de los tres días de la solicitud.

A su vez, respecto a la Comisión Consultiva, sus cometidos se definen a través del siguiente elenco (art. 20):

a) asistir y asesorar a las personas que lo requieran;
b) asistir y asesorar preceptivamente al Ministerio de Economía y Finanzas en el dictado de reglamentos y resoluciones referentes a las actividades comprendidas en la ley;
c) llevar un registro permanente y actualizado de los archivos, registros, bases de datos o similares;
d) controlar la observancia de las normas sobre la integridad, veracidad y seguridad de los datos personales de carácter comercial por parte de los responsables de las bases de datos;
e) emitir opinión toda vez que le sea requerida por las autoridades competentes, incluyendo solicitudes relacionadas con el dictado de sanciones administrativas; y
f) tener presente, en lo que fuere pertinente, las resultancias de las acciones de habeas data.

[42] DELPIAZZO, Carlos E. *"Desafíos actuales del control"*, F.C.U., Montevideo, 2001, pp. 8 y ss.

La sola descripción de los cometidos atribuidos a la Comisión Consultiva -que será un cuerpo de funcionamiento no permanente sino periódico- evidencia que el Ministerio de Economía y Finanzas deberá montar una oficina especializada para llevar a cabo las tareas que la ley encomienda a dicha Comisión, que no son sólo de consulta y asesoramiento sino también activas.[43]

Durante la discusión parlamentaria[44], los aspectos referidos al control administrativo fueron los más debatidos en el Senado, oportunidad en la cual se cuestionó tanto la implantación del órgano de control (planteándose alternativamente el Ministerio de Educación y Cultura por su competencia en materia registral y de derechos humanos) como su estatuto jurídico (en cuanto a la necesidad de dotarlo de autonomía técnica, al estilo de las Unidades Reguladoras actualmente existentes).

La opción aprobada estuvo respaldada en una visión de la ley centrada en la protección del consumidor. No obstante, si bien dicha perspectiva no es equivocada, creo que es fácil coincidir en que el Ministerio de Economía y Finanzas no es el órgano más idóneo para cumplir una tarea de relevante importancia en la tutela de un derecho fundamental de última generación.

Sobre el particular, el Derecho comparado exhibe múltiples antecedentes de configuración de órganos u organismos creados con independencia técnica y funcional como modo de garantizar de mejor modo el derecho fundamental en juego. Así, la Directiva del Parlamento Europeo y del Consejo Nº 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos, establece en su art. 28, num. 1º que "Los Estados miembros dispondrán que una o más autoridades públicas se encarguen de vigilar la aplicación en su territorio de las disposiciones adoptadas por ellos en aplicación de la presente Directiva. Estas autoridades ejercerán las funciones que les son atribuidas con total independencia".[45]

Incluso entre nosotros, los antecedentes resultantes de la creación de las Unidades Reguladoras de los Servicios de Comunicaciones (URSEC) y de los Servicios de Energía y Agua (URSEA) evidencian la preocupación por dotarlas de una autonomía técnica acorde a la importancia de su actividad regulatoria y de control.[46]

VII. Conclusión

La sola aprobación de una ley -aunque importante- no agota la labor constructiva de los operadores del Derecho, sobre todo cuando, como ocurre en la especie, nos encontramos en el campo tutelar de los derechos fundamentales inherentes a la personalidad.

[43] Delpiazzo, Carlos E. *"Bases conceptuales de la organización administrativa uruguaya"*, en Rev. de Administración Pública Uruguaya, Nº 22, pp. 61 y ss.

[44] Ver: Diario de Sesiones de la Cámara de Senadores correspondiente al 8 de junio de 2003, pp. 274 y 275.

[45] Heredero Higueras, Manuel. *"La Directiva Comunitaria de Protección de los Datos Personales"* (Aranzadi, Pamplona, 1997), pp. 201 y ss.

[46] Delpiazzo, Carlos E. *"Régimen jurídico de las telecomunicaciones"*, U.M., Montevideo, 2001, pp. 38 y ss.; y "Desafíos actuales del control" cit., pp. 27 y ss.

Por eso, en el estado actual de cosas, es preciso apostar a la jurisprudencia administrativa que vaya acuñando la Comisión Consultiva y a su preceptiva intervención en la reglamentación a dictarse.

Igualmente, es de esperar que la nueva ley ambiente un desarrollo de la jurisprudencia judicial en la línea de la mejor defensa de los derechos en juego.