
MARCELA BASTERRA



**EL HÁBEAS DATA:
LA REFORMA CONSTITUCIONAL DE
1994 Y LA SANCIÓN DE LA LEY 25.326
DE PROTECCION DE DATOS PERSONALES
Y DE HÁBEAS DATA**

**EL HÁBEAS DATA:
LA REFORMA CONSTITUCIONAL
DE 1994 Y LA SANCIÓN DE LA
LEY 25.326 DE PROTECCIÓN
DE DATOS PERSONALES
Y DE HÁBEAS DATA**

RESUMEN

El artículo tiene por objeto analizar a garantía de *hábeas data* partiendo de los antecedentes extranjeros; comparando la fórmula constitucional argentina con la de otros países. Se establecen de acuerdo con la doctrina y jurisprudencia nacional el objeto, la finalidad y los derechos tutelados por el instituto. Se realiza una análisis de la Jurisprudencia más importante de Argentina; demostrando cómo la Ley Reglamentaria 25.326, del artículo 43 de la Constitución Nacional toma los principios básicos sentados por la jurisprudencia y la doctrina; tal el caso de la ampliación de la legitimación, la creación pretoriana del derecho a la verdad objetiva, y los límites al secreto de Estado.

I. ANTECEDENTES EXTRANJEROS A LA INCORPORACIÓN DEL *HÁBEAS DATA* EN LA CONSTITUCIÓN ARGENTINA¹

La acción de *hábeas data* tal y con ese nombre tiene su antecedente en la constitución de Brasil de 1988 que en su artículo 5 inciso LXXII establece

«Conceder el *hábeas data*: a) para asegurar el conocimiento de informaciones relativas a la persona de quien lo pide, que conste en registro o banco de datos de entidades gubernamentales o de carácter público, b) para la rectificación de datos cuando no se prefiera hacerlo por proceso reservado judicial o administrativo».

Esta norma a su vez toma como fuente la Ley 824 de 1984 del estado de Río de Janeiro.

Sin embargo, ya había normas supranacionales que protegen el derecho a la intimidad; así, v. gr., la *Declaración de los Derechos del Hombre de la Asamblea General de las Naciones Unidas* de 1948, cuyo artículo. 12 establece... «nadie puede ser objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio, correspondencia...»; la *Declaración Americana de Derechos y Deberes del Hombre*, suscripta en Bogotá en 1948; y *El Pacto de San José de Costa Rica* en su artículo 11 inciso 2 establece que «nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia...»; todas ellas incorporadas a nuestra Constitución con la reforma de 1994, artículo 75 inciso 22.

1. Ampliar de PUCCINELLI, Óscar, *El hábeas data en Indolberoamérica*, Temis, Santa Fe de Bogotá, Colombia, 1999.

En la Constitución de *Perú* de 1993 se encuentra contemplado en el inciso 3 del artículo 200 «La acción de *hábeas data* que procede contra el hecho u omisión, por parte de cualquier autoridad, funcionario o persona, que vulnere o amenaza los derechos a que se refiere el artículo 2 incisos 5, 6 y 7 de la constitución», que respectivamente aluden al «*hábeas data* exhibitorio, o sea, a poner en conocimiento de la persona que interpone el *hábeas data* de los datos a ella referidos (inciso 5); se prevé el no suministro de informaciones que afecten la intimidad personal y familiar (inciso 6) y por último el *hábeas data* que tenga en miras asegurar los derechos al "honor y buena reputación, intimidad personal y familia, voz e imagen propias"².

La Constitución de *Colombia* de 1991 en su artículo 15 establece:

«Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre y el Estado tiene que respetarlos y hacerlos respetar. De igual modo tiene derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en banco 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...».

La Constitución del *Paraguay* de 1992, dice en su artículo 135

«Toda persona podrá acceder a la información y a los datos que sobre la misma y sobre sus bienes obren en registros oficiales o de carácter público, así como conocer el uso que se haga de los mismos y su finalidad. Podrá solicitar ante el magistrado competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afecten ilegítimamente sus derechos».

También ha recogido esta normativa la Constitución de *Guatemala*, que en su artículo 31 expresa

«Toda persona tiene derecho a conocer lo que de ella conste en archivos, fichas o cualquier otra forma de registros y archivos de filiación política, excepto los propios de las autoridades electorales y de los partidos políticos».

La Constitución de *México* en su artículo 7 consagra la libertad de imprenta y consagra como límites a la moral, la paz pública y el respeto a la vida privada. También hay una llamada "Ley de Información Estadística y Geográfica", publicada en el *Diario Oficial* el 30/12/1980 que constituye una herramienta básica en el manejo de la informática, en su artículo 5 asegura la confidencialidad a los informantes y ordena la producción de reglas que regulará el acceso del público a la información. El artículo 32 establece la

2. SAGÜÉS, Néstor Pedro, "Subtipos de *hábeas data* en el Derecho argentino. Sus posibilidades en el peruano", *Leyes Reglamentarias de la Reforma Constitucional*, Asociación Argentina de Derecho Constitucional, noviembre de 1996, p. 212.

obligación general de contribuir con la secretaría a todo el proceso de captar, producir, procesar, y divulgar información³.

En los Estados Unidos rige la *Privacy Act* de 1974. La jurisprudencia de la Corte Suprema de Justicia de los Estados Unidos distingue según que el recabamiento de datos parte del gobierno o de un particular; en el primer caso ha sostenido, en el caso «Talley vs. California» 362 U.A. 345 (1970), que el derecho a la privacidad no es obstáculo para que el Estado pueda ejercer su derecho de recopilar datos relativos a personas particulares, con algunas excepciones. Sin embargo, si el recabamiento de datos parte de un particular, ha sostenido, en el caso «Detroit Edison Co. vs. NLRB» 440 U.S. 301 (1979), un criterio restrictivo, incluso cuando se trata del uso de datos por medio de la prensa C.S.E.U. 436 U.S. 547 (1978), 420 U.S. 469 (1975)⁴.

En 1968, en la *Conferencia Internacional de Derechos Humanos*, realizada en Teherán queda establecido el riesgo que implican los avances tecnológicos y científicos en lo que pudieran afectar los derechos humanos, y la Asamblea General de la ONU recomienda a los Estados la realización de estudios con miras al dictado de normas que protegieran adecuadamente las libertades individuales, especialmente «las aplicaciones de la electrónica que puedan afectar los derechos de las personas y los límites que deberían fijarse para estas aplicaciones en una sociedad democrática». En ese mismo año el Consejo de Europa, a través de su Comité de Ministros, llevó adelante un estudio sobre la normativa de la Convención Europea de los Derechos del Hombre, con el fin de investigar si en los Estados miembros existía una protección de la privacidad y demás derechos conexos en relación con los avances tecnológicos y científicos. Cumpliendo con estas disposiciones del Comité de Ministros del Consejo de Europa en 1976, un grupo de expertos elabora el texto de lo que fue la Convención para la protección de los individuos con relación al procesamiento automático de datos personales, conocida como la *Convención de Estrasburgo* y suscripta por veintiún Estados europeos⁵.

La Constitución de *Portugal* de 1976 expresa en su artículo 35

«Todos los ciudadanos tienen el derecho de informarse sobre los contenidos de los bancos de datos que le[s] conciernen y sobre el uso que se les pretenda asignar. Están autorizados para exigir que esos contenidos sean corregidos y actualizados. Los datos no podrán ser utilizados para suministrar información concerniente a las convicciones políticas de las personas, religiosas o relacionadas con la vida privada con la excepción de que su uso responda a propósitos estadísticos y que no permitan la individualización de la persona. Los ciudadanos no podrán ser individualizados con número de identificación en la documentación nacional».

3. MEJÁN, Luis Manuel, *El derecho a la intimidad y la informática*, Porrúa, México, 1996, p. 112.

4. EKDMEKDJIAN, Miguel Ángel, «El *habeas data* en la Reforma Constitucional», *La Ley*; 15 de noviembre de 1995, suplemento, pág. 42.

5. ALTMARK, Ricardo D. y MOLINA QUIROGA, Eduardo, *Habeas data*, *La Ley*, T. 1996-A, pp., 1157-1158.

Si bien en este caso no se refiere específicamente a una acción determinada, quedan claramente protegidos el derecho a la privacidad de las personas y sus datos personales⁶. Asimismo, está legislado el *hábeas data* en *Alemania* (1977), *Austria*, *Luxemburgo*, la *Data Lag* de Suecia (1970) y Francia (1978).

En el *Reino Unido* rige a partir de 1984⁷, también en *Australia*, *Bélgica*, *Italia*, *Finlandia* e *Islandia*. Es de gran importancia en orden a esta legislación el Convenio para la protección de personas respecto al tratamiento automatizado de datos de carácter personal, adoptado por el Comité de Ministros del Consejo de Europa (1980). Este texto, entre otros preceptos, establece la exigencia de veracidad y correcta utilización de datos (artículo 5), prohíbe el tratamiento automático de informaciones referentes al origen racial, opiniones políticas, creencias religiosas u otras, salud sexual y condenas penitenciarias (artículo 6). Se reconoce el derecho de los interesados a conocer los datos existentes en relación con su persona, la posibilidad de cancelarlos o corregirlos... (artículo 8)⁸.

El caso de *España* merece una mención aparte. En este país se ha generado gran preocupación en relación con el tema de los datos personales frente al uso de la informática, y hay estudios exhaustivos acerca del denominado "derecho a la autodeterminación informativa"⁹. Se incorpora en la Constitución de 1978 (artículo 18.4 y 105b). En 1992, se sanciona la "Ley Orgánica de Regulación del Tratamiento Automatizado de Datos", en cuyo artículo 1 protege a las personas físicas (no así a las jurídicas) contra la divulgación de sus datos de carácter personal que consten en cualquier registro automatizado de datos. También prevé en su artículo 6.1 que "el tratamiento automatizado de los datos requerirá el consentimiento del afectado, salvo que la ley disponga otra cosa", el cual asimismo es susceptible de revocación, y no requiere ser expresado bajo ninguna formalidad específica. En relación con los medios legales con que cuenta el titular de los datos, la ley le otorga los siguientes derechos: acceso al registro (artículo 14), derecho de rectificación y cancelación de los mismos (artículo 15); y también se prevé el derecho del afectado a la impugnación de actos administrativos o acciones de particulares que puedan tender a descalificar a una persona con base en los datos de ella recopilados (artículo 12)¹⁰. Es importante lo que ha generado la legislación española y la doctrina en relación con la protección de los denominados "datos sensibles", que se refieren a las creencias religiosas, orientación sexual, ideología política, estado de salud del afectado, etc. Para estos casos la ley prevé que se preste por escrito el consentimiento del interesado.

6. BIANCHI, Alberto B., *Hábeas data y derecho a la privacidad*. E.D.: 16 de febrero de 1995, p. 1.

7. GOZAINI, Osvaldo, *El derecho de amparo*. Depalma, Buenos Aires, 1995, p. 162.

8. SABSAY, Daniel A. y ONAINDIA, José M. *La Constitución de los argentinos*. Errepar, Buenos Aires, 1997 pp. 157-158.

9. MURILLO DE LA CUEVA, Pablo Lucas, «La protección de los datos personales ante el uso de la información en el derecho español», *Estudios de Jurisprudencia de Madrid*, revista *Colex*, Madrid, 1993, año II, n. 4. Citado por BIANCHI, Alberto B., *op. cit.*, p. 10.

10. EKMEKIDJIAN, Miguel Ángel, *op. cit.*, p. 42

Si bien todos los ordenamientos preferidos han acogido esta garantía, hay algunas diferencias que merecen ser remarcadas. Con relación al bien jurídico protegido, algunos ordenamientos hacen hincapié en la fe religiosa, convicciones política, y a la vida privada (Portugal); otras en el honor y la intimidad (España); intimidad personal y familiar y al buen nombre (Colombia); a la filiación política (Guatemala).

Las primeras constituciones en abordar específicamente el tema de la problemática generada sobre la explosión informática, fueron, sin duda, las de España y Portugal.

La normativa constitucional en algunos países sólo contienen un marco general, para que posteriormente el poder legislativo haga las reglamentaciones necesarias (España); otras sin embargo son más reglamentaristas detallistas, estableciendo concretamente los derechos de los registrados (Portugal, Brasil, Paraguay, Colombia).

En torno al acceso a los propios datos, el conocimiento de los datos volcados en los registros y la finalidad con que serán usados; hay constituciones que lo contemplan expresamente (Portugal, Colombia, Guatemala, Paraguay). Respecto del sujeto que puede solicitar el acceso algunas leyes lo prevén para toda persona registrada (físicas y jurídicas) (Perú, Brasil, Paraguay, Colombia, Guatemala).

En relación con la posibilidad de solicitar la supresión, rectificación, confidencialidad o actualización de los datos, también podemos hacer algunas diferenciaciones. Si se trata de datos inexactos, el afectado tendrá derecho a solicitar por esta vía la actualización de los mismos (Portugal, Brasil, Colombia). Algunas constituciones prevén la actualización de datos y la exclusión o supresión de los mismos (Paraguay). Por último, agregaremos que algunas legislaciones establecen el control de la finalidad, propósito o destino de los datos (Portugal, Paraguay, Guatemala)¹¹.

II. EL HÁBEAS DATA EN LA CONSTITUCIÓN ARGENTINA

El artículo 43¹² de nuestra Constitución se refiere al amparo, en el primer párrafo; al amparo colectivo, en el segundo párrafo, y en el tercer párrafo

11. PUCCINELLI, Óscar Raúl. "Reflexiones ante la inminente reglamentación del hábeas data", *Boletín Informativo de la Asociación Argentina de Derecho Constitucional*, n. 133, mayo de 1997, pp. 7-10.

12. Artículo 43. Toda persona puede interponer acción expedita y rápida de amparo, siempre que no exista otro medio judicial más idóneo, contra todo acto u omisión de autoridades públicas o de particulares, que en forma actual o inminente lesione, restrinja, altere o amenace, con arbitrariedad o ilegalidad manifiesta, derechos y garantías reconocidos por esta Constitución, un tratado o una ley. En el caso, el juez podrá

incorporó la acción de *hábeas data* sin mencionarlo en forma expresa; como un subtipo de amparo; con la siguiente fórmula:

«...Toda persona podrá interponer ésta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que conste en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad, o actualización de aquéllos. No podrá afectarse el secreto de las fuentes de información periodística».

La norma resulta sumamente clara cuando establece en el primer párrafo: «Toda persona puede interponer acción expedita y rápida de amparo...»; y en el tercer párrafo: «Toda persona podrá interponer ésta acción para tomar conocimiento de los datos a ella referidos...»; de la interpretación de la norma no cabe duda de que está planteado como una subespecie de amparo o amparo especial como lo ha considerado la doctrina mayoritaria.

Planteamos nuestras dudas acerca del real convencimiento del Constituyente de introducir esta garantía en la Constitución Nacional como especie de amparo, y no como una acción independiente; ello es así porque en la Ley 24.309 que declaró la necesidad de reforma en los temas habilitados del artículo 3 punto "N" se mencionaba la "consagración expresa del *hábeas corpus* y del amparo", mediante la "incorporación de un artículo nuevo en el Capítulo Segundo de la Primera Parte de la Constitución Nacional"; el que conocemos ahora como "Nuevos Derechos y Garantías"; de manera que ante tan importante "olvido", la única manera posible era introducir este instituto jurídico en nuestra Carta Magna como un subtipo de amparo. Lo cierto es que sean reales o imaginarios estos motivos, de la propia letra de la Constitución surge que el *hábeas data* es procesalmente una acción de amparo que procede cuando no hay un medio judicial más idóneo.

En este sentido ha sido interpretado por la Jurisprudencia puesto que si analizamos las sentencias dictadas hasta el momento, observamos que todos se refieren a una "acción de amparo", a partir del fallo "García de Llanos Isabel c/Caja de Jubilaciones, Pensiones y Retiros de Córdoba s/*hábeas data*" del 29/3/95 la Cámara Contencioso Administrativa de Córdoba

declarar la inconstitucionalidad de la norma en que se funde el acto u omisión lesiva. Podrán interponer esta acción contra cualquier forma de discriminación y en lo relativo a los derechos que protegen al ambiente, a la competencia, al usuario y al consumidor, así como a los derechos de incidencia colectiva en general, el afectado, el defensor del pueblo y las asociaciones que propendan a esos fines, registradas conforme a la ley, la que determinará los requisitos y formas de su organización. Toda persona podrá interponer esta 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 aquellos. No podrá afectarse el secreto de las fuentes de información periodística. Cuando el derecho lesionado, restringido, alterado o amenazado fuera la libertad física, o en caso de agravamiento ilegítimo en la forma o condiciones de detención, o en el de desaparición forzada de personas, la acción de *hábeas corpus* podrá ser interpuesta por el afectado o por cualquiera en su favor y el juez resolverá de inmediato, aun durante la vigencia del estado de sitio.

estableció «la acción de *hábeas data* es una modalidad de amparo que permite a toda persona interesada a acceder al conocimiento de los datos...».

La novel Ley de Protección de Datos Personales y *hábeas data* 25.326, publicada en el *Boletín Oficial* el 2 de noviembre de 2000; crea una "acción Judicial de amparo especial", que es la que toma el nombre de *hábeas data*. El artículo 33 (Procedencia) expresa:

«1. La acción de protección de los datos personales o de *hábeas data* procederá: a) para tomar conocimiento de los datos personales almacenados en archivos, registros o bancos de datos públicos o privados destinados a proporcionar informes, y de la finalidad de aquéllos; b) en los casos en que se presuma la falsedad, inexactitud, desactualización de la información de que se trata, o el tratamiento de datos cuyo registro se encuentra prohibido en la presente ley, para exigir su rectificación, supresión, confidencialidad o actualización».

Complementaria de esta disposición es el

«Artículo 37. (Procedimiento aplicable). La acción de *hábeas data* tramitará según las disposiciones de la presente ley y por el procedimiento que corresponde a la acción de amparo común y supletoriamente por las normas del Código Procesal Civil y Comercial de la Nación, en lo atinente al juicio sumarísimo».

De manera que es la ley la que, continuando lo establecido desde la constitución y la jurisprudencia, toma la garantía de *hábeas data* como "acción de amparo especial". Si del artículo 33 queda alguna duda es despejada completamente por el artículo 37.

III. FINALIDAD Y OBJETIVOS DEL HÁBEAS DATA

El *hábeas data* es un instituto que podríamos relacionarlo con el concepto de postmodernidad jurídica, puesto que es relativamente reciente y lo vinculamos con la denominada "explosión informática" y la consecuente multiplicación de archivos, registros y bancos de datos.

Constituye una garantía que tiende a que todos puedan acceder a las constancias de los archivos para poder controlar su veracidad y difusión¹³.

«El *hábeas data* tiene por finalidad impedir que en bancos o registros de datos se recopile información respecto de la persona titular del derecho que interpone la acción, cuando dicha información esté referida a aspectos de su personalidad que se encuentren directamente vinculados con su intimidad, no correspondiendo encontrarse a disposición del público o ser utilizados en su perjuicio por órganos

13. COLAUTTI, Carlos E., *Reflexiones preliminares sobre el hábeas data*, LL 1996-C, p. 917.

públicos o entes privados, sin derecho alguno que sustente dicho uso. Se trata particularmente de información relativa a la filiación política, ideas religiosas, militancia gremial, desempeño laboral participación académica, etc. Las tristes experiencias de persecución ideológica vividas en el país justifican plenamente la tutela»¹⁴.

Toda persona que vive en una sociedad tecnológica desarrollada, a diario, da determinada información acerca de sí misma, de sus datos, domicilio, número de documento, profesión, miembros que integran su familia, si posee tarjetas de créditos, si tiene cuenta bancaria, si tiene automóvil, estudios cursados, datos relacionados con su patrimonio, si milita en un partido político, sus creencias religiosas, etc.; todo ello susceptible de ser guardado en archivos o bancos de datos con la potencialidad de ser utilizado con fines discriminatorios o simplemente en forma indebida. Es más: si se entrecruzan esos datos arroja un perfil completo de la persona, una verdadera "radiografía". Sin duda, la protección de las personas contra el uso abusivo de la informática, que violente derechos fundamentales como el de la intimidad, el honor, a la imagen, etc., es uno de los fines fundamentales que tuvo en miras el legislador al establecer esta garantía.

Tomando los fines y objetivos de la letra de la norma constitucional, la Cámara Nacional de Apelaciones en lo Contencioso Administrativo Federal de la Capital Federal estableció en autos "Farrel Desmond Agustín c/ B.C.R.E.A. y otros s/ Amparo" (sent. 5/9/1995) y ratificó en autos "Gaziglia, Carlos Raimundo y otro c/ B.C.R.A. y otro s/ Amparo" (sent. 4/10/1995):

«El *hábeas data* tiene cinco objetivos principales: a) que una persona pueda acceder a la información que sobre ella conste en un registro o banco de datos; b) que se actualicen datos atrasados; c) que se rectifiquen datos inexactos; d) que se asegure la confidencialidad de cierta información legalmente obtenida para evitar su conocimiento por terceros; e) supresión del registro de la llamada "información sensible"-vida íntima, ideas políticas, religiosas o gremiales».

Respecto a los objetivos del instituto la doctrina mayoritaria es conteste en considerar en más o en menos estos prerreferidos objetivos.

Consideramos que esta garantía tiene una finalidad inmediata, que está comprendida en la posibilidad que tienen las personas de "...tomar conocimiento de los datos a ella referidos y de su finalidad..."; y de una finalidad mediata, en cuanto que si dichos datos resultan "falsos o discriminatorios podrá exigir la supresión, rectificación, confidencialidad o actualización de los mismos". Si bien la letra del artículo 43 se refiere sólo a los datos "falsos o discriminatorios", creemos que quedan equiparados

14. HITTERS, Boletín n. 26, p. 1260, cit. por QUIROGA LAVIÉ, *El amparo, el hábeas data y el hábeas corpus*, p. 157. Ed. Rubinzale-Culdoni, Buenos Aires, 1995.

también los datos antiguos u obsoletos, y los llamados "datos sensibles" que son los relacionados con ideas políticas, creencias religiosas, orientación sexual, no siendo necesarios que sean falsos o que vayan a utilizarse con fines discriminatorios, sólo basta con que por el tipo de datos que son, se considere que pertenecen a la más absoluta intimidad de las personas y que no tienen por qué ser de público conocimiento. No siendo necesario asimismo que se produzca un daño a la persona titular de los datos. En el mencionado fallo "Gaziglia C. y otro c/ B.C.R.A. y otros") el *a quo* también dejó establecido que

«...para la procedencia del *hábeas data* no se requiere en principio arbitrariedad o ilegalidad manifiesta...dado que procede ante la mera falsedad de dichos datos o la discriminación que de ellos pudiere resultar y aún solo para conocer dichos datos, sin que sea necesario que ellos vulneren derechos o garantías constitucionales».

Por todo ello y teniendo en cuenta que dividimos los fines en inmediatos y mediatos, coincidimos con la clasificación que hace Sagués en cuanto a los tipos de *hábeas data* en relación al objetivo concreto planteado.

Para cumplir con los que hemos llamado fines inmediatos contamos con el denominado:

1. *Hábeas data informativo* que nos permitirá conocer: a) qué datos se poseen acerca de mi persona –*hábeas data exhibitorio*–; b) cuál va a ser la finalidad de dichos datos, el uso que se les va a dar –*hábeas data finalista*–; c) quién recopiló esos datos –*hábeas data autoral*–, lo que será importante para determinar la procedencia o no de la acción; por ejemplo, si los datos fueron adquiridos de fuentes de información periodísticas.

Para el cumplimiento de los fines mediatos y según el caso concreto, tenemos:

2. *Hábeas data aditivo*: por medio de esta acción solicitamos que se agregue un dato que no está en el registro o banco ante el que iniciamos la misma. Es la "actualización" la que se refiere el artículo 43 de la Constitución Nacional.
3. *Hábeas data rectificador*: se interpone para el caso que se trate de un dato "falso" en los términos constitucionales, "rectificación", solicitamos se cambie por el dato verdadero.
4. *Hábeas data reservador*: está previsto para los casos en que el dato sea verdadero y que no hay obstáculos para la conservación del mismo. Sin embargo, el juez interviniente puede ordenar al banco de datos su "confidencialidad", para uso estrictamente personal o específico; también está expresamente contemplado en nuestra Constitución.

5. *Hábeas data cancelatorio*: el artículo 43 también prevé la "supresión" de datos, para evitar que sean usados con fines discriminatorios o en forma abusiva; se refiere a los que hemos llamado "datos sensibles"¹⁵.

Es de destacar que en el convenio 108 sancionado por el Consejo de Europa en 1981, que trata de enumerar cuáles son los denominados "datos sensibles", explica que estos datos son: el origen social de la persona, sus opiniones políticas, militancia y participación gremial, si tiene o no convicciones religiosas, datos referidos a la salud y a la vida sexual, las condenas judiciales o penales de que hubiera sido pasible.

«Este conjunto de datos, lo son, precisamente con ese calificativo de sensibles, porque el manipuleo o manejo de ellos puede ocasionar –como en el circo romano– la muerte de una persona. La muerte civil, la muerte de su prestigio...»¹⁶.

Con respecto a los datos protegidos por esta garantía en el artículo 43, la nueva ley ha tomado lo establecido desde la Jurisprudencia y la Doctrina, ya que la Constitución sólo menciona los datos "falsos o discriminatorios"; y la ley es sumamente clara cuando establece la procedencia en el artículo 33, b) para los casos que se presume «falsedad, inexactitud, desactualización, o datos cuyo tratamiento prohíbe la siguiente ley». A ellos se refieren los artículos 7° y 8°

«**Artículo 7°** (*Categoría de datos*) 1. Ninguna persona puede ser obligada a proporcionar datos sensibles. 2. Los datos sensibles sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley. También podrán ser tratados con finalidades estadísticas o científicas cuando no puedan ser identificados sus titulares. 3. Queda prohibida la formación de archivos, bancos o registros que almacenen información que directa o indirectamente revele datos sensibles. Sin perjuicio de ello, la Iglesia católica, las asociaciones religiosas y las organizaciones políticas y sindicales podrán llevar un registro de sus miembros. 4. Los datos relativos a antecedentes penales o contravencionales sólo pueden ser objeto de tratamiento por parte de las autoridades públicas competentes, en el marco de las leyes y reglamentaciones respectivas».

«**Artículo 8°** (*Datos relativos a la salud*). Los establecimientos sanitarios públicos o privados y los profesionales vinculados a las ciencias de la salud pueden recolectar y tratar los datos personales relativos a la salud física o mental de los pacientes que acudan a los mismos o que estén o hubieren estado bajo tratamiento de aquéllos, respetando los principios del secreto profesional».

15. SAGÜES, Néstor Pedro, "Subtipos de *hábeas data* en el Derecho argentino". *Leyes Reglamentarias de la Reforma Constitucional*, Asociación Argentina de Derecho Constitucional, Buenos Aires 1996, pp. 206-208.

16. VANOSSE, Jorge Reinaldo, *op. cit.*, p. 951.

IV. DERECHOS TUTELADOS¹⁷

Se torna engorroso abordar este tema si tenemos en cuenta que la doctrina está dividida en cuanto a los derechos tutelados por esta garantía, es imposible hacer una clasificación taxativa de las distintas posturas, pero a grandes rasgos podemos decir:

A. Doctrina

1. Gran parte de la doctrina reconoce como bien jurídico tutelado el *derecho a la intimidad*, en primer lugar y otros conexos a él. Dentro de esa postura se enrolan los siguientes autores:

Bianchi nos dice que sin perjuicios de otros, los derechos protegidos por el *hábeas data* son: la *privacidad*, la *identidad* y el *honor* de una persona¹⁸; **Ekmekdjian** considera que el fundamento del *hábeas data* es la protección de la *intimidad* de las personas y a su *privacidad*, siendo estos últimos una derivación del derecho a la dignidad¹⁹; **Sagués** también se refiere al honor o la *privacidad*²⁰; **Falcón** dedica varias páginas de su libro *Hábeas data* a explicar que esta garantía protege el derecho a la intimidad y protege a las personas de la discriminación. **Badeni**²¹ también hace mención al *derecho a la intimidad o privacidad* como al honor. **Dromi** y **Menem** reconocen el fundamento de esta garantía también en el derecho a la *intimidad*, aclarando que se halla integrado por la *tranquilidad*, la *autonomía* y el *control de la información personal*²². **Quiroga Lavié, Natale, Antonio Hernández** y **Palazzi** también se refieren a la *intimidad* y a la *privacidad* como bienes jurídicos protegidos por esta garantía.

2. Otro grupo de doctrinarios posee una visión ampliada hacia una gama de otros derechos; tal el caso de **Puccinelli** que considera que en primer lugar se tutela el derecho a la *intimidad* y como consecuencia de ello afecta otros derechos a la *integridad física, psíquica*, el *derecho a trabajar*, etc., y en segundo lugar el permitir accionar sobre datos falsos, el *valor verdad* y toda la gama de afecciones a otros derechos que por vía de esa falsedad puede sufrir la persona, como serían el *honor*, la *reputación*, la *imagen*, la *identidad*, etcétera²³.

17. Ampliar de DALLA VIA, Alberto-BASTERRA, Marcela, *Hábeas data y otras garantías constitucionales*; Némesis, Buenos Aires, 1998, pp. 11-120

18. BIANCHI, Alberto B., op. cit. p. 6.

19. EKMEKDJIAN, Miguel A., «El *hábeas data* en la Reforma Constitucional»; *La Ley*, 1995-E. Buenos Aires, p. 946.

20. SAGUÉS, Pedro Néstor, «Amparo, *Hábeas data* y *hábeas corpus* en la reforma constitucional»; *La Ley*, 1994-D, p. 1158.

21. BADENI, Gregorio, *Reforma Constitucional e Instituciones Políticas*, Buenos Aires, 1994, p. 247.

22. DROMI, Roberto y MENEM, Eduardo, op. cit., p. 168.

23. PUCCINELLI, Óscar Raúl, «Reflexiones ante la inminente reglamentación del *hábeas data*». *Boletín Asociación Argentina de Derecho Constitucional*, n. 134, p. 8

En su calidad de convencional-constituyente de 1994 **Cullén** sostuvo que “es tan importante que precisemos que este derecho o garantía jurisdiccional... que estamos dando a la gente para que defienda su derecho a la *reputación* y a la *honra* –porque eso es lo que defiende el *hábeas data*–, no va a ir, desde ningún punto de vista en desmedro de la *privacidad* y el *secreto profesional* que puedan tener otros”²⁴. Según **Bidart Campos**, el *hábeas data* tiene como fin principal el evitar el *abuso informático*, pero no necesariamente dicho abuso tiene que existir, pues también se tiene en miras preservar en la confidencialidad y la reserva de bienes personales como los que hacen a la *dignidad*, el *honor*, la *privacidad*, la *información sensible*, la *autodeterminación informática*, la *igualdad*, etc.²⁵. **Vanossi** nos habla de la protección de la identidad informativa de la persona, siguiendo a Alfonso Da Silva; y de la protección de lo más inherente a la propia persona, que es el derecho a su perfil y el derecho a su *imagen*²⁶. El convencional-constituyente **Díaz**, en su calidad de miembro informante del despacho de la mayoría –creemos–, generalizó en exceso al considerar que el *hábeas data* serviría para proteger la *libertad* y otros derechos personales de los argentinos.

3. **Bazán** deja sentada su propia postura en el sentido de considerar que esta nueva garantía constitucional es el reflejo de la necesidad de abrir camino a un «nuevo derecho o al menos a la reformulación de uno clásico cuyos contornos se han visto desbordados o erosionados por la realidad»; se refiere al derecho a la *autodeterminación informativa*. «El *hábeas data* brinda cauce de tutela a la libertad informática, que da pie a la existencia de un derecho autodeterminativo que va ganando adeptos en la doctrina y jurisprudencia europeas...». Nos cita una sentencia del Tribunal Constitucional Federal Alemán (15/12/1983) en la que se declaró parcialmente inconstitucional la ley germana del censo de población de 1982, y siguiendo a Pérez Lueño se establece el mérito de la sentencia en haber entendido el derecho a la intimidad como el derecho a la autodeterminación informativa, como la facultad de la persona de «decidir básicamente por sí misma cuándo y dentro de que límites procede revelar situaciones dentro de la propia vida»²⁷. Como lo destacamos en párrafos anteriores, Bidart Campos, al mencionar el plexo de derechos cuya garantía es el *hábeas data*, menciona la *autodeterminación informativa*.

24. Citado por PUCCINELLI, Óscar, *op. cit.*, p. 12.

25. BIDART CAMPOS, Germán, *Manual de la Constitución Reformada*, t. II, Ediar, Buenos Aires, 1997, p. 389.

26. VANOSI, Jorge Reinaldo, *op. cit.*, p. 954.

27. PÉREZ LUEÑO, Antonio E., citado por BAZÁN, Víctor, «El *hábeas data* y la custodia al derecho a la autodeterminación Informativa”. *Boletín Asociación Argentina de Derecho Constitucional*, n. 142, p. 9, febrero de 1998.

B. Derecho constitucional provincial

También en las normas de nuestro derecho público provincial hay divergencia en relación a los derechos tutelados por esta garantía constitucional. Genéricamente y a modo de ejemplo, podemos dividirlos en dos grandes grupos:

1. Algunas provincias se refieren a este instituto, enmarcándolo dentro del derecho al acceso a las fuentes de información, para actualizar, suprimir, rectificar o exigir confidencialidad de los registros o bancos de datos, pero hacen mención de los derechos tutelados; **Córdoba** (art. 50); **Buenos Aires** (art. 20); **La Rioja** (art. 30); **Río Negro** (art. 20); **Jujuy** (art. 23); **San Juan** (arts. 26 y 27) –*honor, intimidad personal y familiar, vida privada y el pleno ejercicio de los derechos*.
2. Otras provincias se refieren al derecho de acceso a las fuentes de información; para actualizar, suprimir, rectificar o exigir confidencialidad de los registros o bancos de datos **Tierra del Fuego** (art. 45); **Chubut** (art. 56); **Chaco**; **Formosa** (art. 10); **Catamarca** (art. 11); **San Luis** (art. 21). No se mencionan expresamente los derechos tutelados, surgen de la interpretación doctrinaria y jurisprudencial.

En estas circunstancias está la Constitución Nacional (art. 43) y la Constitución de la **Ciudad Autónoma de Buenos Aires** (art. 16)

C. Normas de derecho comparado

Si pasamos una somera revista a las normas sobre *hábeas data* en otros países, tampoco hay uniformidad acerca de los derechos tutelados, *fe religiosa, convicciones políticas y vida privada*; **Portugal** (art. 35); *buen nombre e intimidad personal y familiar*; **Colombia** (art. 15); *honor, intimidad y propia imagen*; **España** (arts. 18 y 20) esos derechos y además *buen reputación, voz e imagen propias*; **Perú** (art. 200); *moral, paz pública y vida privada*; **México** (art. 7), *honor personal*; **Alemania** (art. 5); *intimidad personal*, **Holanda** (art. 10), etcétera²⁸.

Hemos dejado en claro nuestra postura. Sostenemos que el *hábeas data* tutela el derecho a la intimidad, pero no en forma genérica, sino a una especie de intimidad; "la *intimidad informática*" y a través de ella el derecho a la imagen o el propio perfil²⁹.

28. Ampliar de DALA VIA-BASTERRA, *op. cit.* cap. II, pp. 59-85.

29. BASTERRA, Marcela, "Hábeas data: derechos tutelados" *La Ley; Doctrina Judicial*, 1999-3; p. 77.

1. El *hábeas data* tutela el derecho a la Intimidad Informática. «El hombre presenta una dualidad de tendencias instintivas: por un lado el ser humano tiene necesidad de saber y por otra de ocultar» (Luis Manuel Meján). Servan Schreiber nos dice en su obra *El Desafío Mundial*, que en la lucha de selección de las especies vivientes, los vencedores han sido siempre los que disponen de mayor información.

Creemos sin duda que el punto justo se encuentra en establecer el equilibrio entre los derechos conexos con nuestra necesidad de saber y los conexos con nuestra necesidad de ocultar, estableciendo los límites para que dentro de un sistema de garantías como el nuestro el ejercicio de un derecho no vaya en detrimento del ejercicio de otro. Consideramos que el derecho a manejar información y el derecho a preservar una esfera de intimidad tienen fundamento en primer lugar en la propia naturaleza humana por ello constituyen Derechos Fundamentales que deben ser garantizados y regulados por el Estado.

La informática es sin duda uno de los grandes descubrimientos del siglo, que utilizada por la administración pública y por las empresas privadas proporciona entre otras cosas eficiencia y eficacia, celeridad a la hora de tomar decisiones o de recabar informaciones, el medio ideal para brindar servicios, tanto públicos como privados, y también el medio propicio para guardar datos de las personas. El encuentro entre informática y administración ha producido una nueva rama del saber, una nueva manera de trabajar.

Debemos tener presente que el uso de la informática en manos tanto del Estado como en manos de los particulares, crea diversos riesgos que pueden suponer una amenaza de agresión a la intimidad de los gobernados o usuarios de servicios.

Resulta interesante traer a colación una encuesta realizada en 1971 por el Younger Committee on Privacy, que cuenta Adoración de Miguel Castaño en su obra *Derecho a la Información frente al derecho a la intimidad*, en la que se preguntaba: ¿Objetaría que se dispusiese de información sobre su...? (los números son el porcentaje de respuestas afirmativas): Vida Sexual 87; Ingresos 78; Historial Médico 51; Opiniones Políticas 42; Número de Teléfono 34; Dirección 33; Opiniones Religiosas 28, etc.

Meján define la intimidad como «el conjunto de circunstancias, cosas, experiencias, sentimientos y conductas que un ser humano desea mantener reservado para sí mismo, con libertad de decidir a quién le da acceso al mismo según la finalidad que persiga, que impone a todos los demás la obligación de respetar y que sólo puede ser obligado a develar en casos justificados cuando la finalidad perseguida por la revelación sea lícita».

Quedan sentados dos principios básicos; el primero: El hombre tiene valores individuales que no pueden ser sacrificados jamás en aras de ningún otro valor, tal el caso del derecho a su propia intimidad; el segundo: Existen casos y circunstancias de excepción en que el valor comunitario, el bien general, debe prevalecer sobre los intereses particulares.

Reconocemos la utilidad y la importancia de la información, pero también es innegable que a veces sentimos amenazada nuestra intimidad. Es necesaria una fórmula de equilibrio, que creemos es el artículo 43 de la Constitución Nacional, que a través de la garantía de *hábeas data* establece: 1) el acceso a las fuentes de información, para conocer los datos que se tengan en relación con la persona; 2) la posibilidad de conocer la finalidad con que se han recabado dichos datos; 3) si dichos datos se consideran falsos o discriminatorios, que a través de la doctrina y la jurisprudencia se hace extensivo a los datos obsoletos y a los llamados "datos sensibles"; 4) se prevé la posibilidad de solicitar la supresión, rectificación, actualización y confidencialidad de los datos.

Queda a nuestro criterio por medio de esta garantía tutelada la intimidad informática de las personas.

Es necesario destacar que bajo ningún punto de vista se pretende rotular de insuficiente la cláusula del artículo 19 de la Constitución Nacional... «las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral pública, ni perjudiquen a un tercero, están solo reservadas a Dios, y exentas de la autoridad de los magistrados...», que nos rige desde 1853 y que dio origen a una jurisprudencia tan rica como variada, contradictoria en algunos casos, cuyas notas más sobresalientes se observan a través de la doctrina sentada por la corte en los fallos "Bazterrica" y "Capalbo" ambos de 1986 sobre tenencia de estupefacientes en los que la Corte cambia la doctrina, para ampliarla en sentido de considerar la tenencia de estupefacientes comprendida en el concepto del derecho a la intimidad del artículo 19 CN. En el caso "Colavini" de 1978 había considerado que la conducta del condenado no se encontraba bajo el ala de protección de las acciones privadas contempladas en el artículo 19 de la Constitución Nacional; para en 1990 en el caso "Montalvo" volver definitivamente a la doctrina "Colavini".

En todos ellos se hace un análisis exhaustivo del derecho a la intimidad; pero es en "Ponzetti de Balbin" de 1984, en el cual la Editorial Perfil fue condenada a indemnizar a la viuda del extinto líder político por el daño moral que le causó la publicación de una foto de su esposo semidesnudo y moribundo en terapia intensiva. En este fallo la Corte estableció el concepto de *derecho a la intimidad* como "el derecho de decidir por sí mismo en qué medios compartirá con los demás, sus pensamientos, sus sentimientos y los hechos de su vida personal". Pensamos que fue un primer paso hacia una especie dentro del género derecho a la intimidad. En definitiva, la nueva garantía lejos de dejar de lado los conceptos desprendidos del artículo 19 en relación con el concepto de intimidad, viene a abonarla estableciendo una especie que es la Intimidad Informática, cuyo fundamento está en la revolución tecnológica e informática producida en los últimos años, para mitigar los efectos de lo que Sagués llama "poder informático" estableciendo un equilibrio que es regla de oro en el derecho constitucional; si hay poder debe haber garantía.

2. El *hábeas data* tutela el derecho a la propia imagen.

Los orígenes de la noción de derecho a la imagen podemos remontarlos al llamado *ius imaginum romano* que alcanza notable importancia durante la República Romana, y que consistía en la práctica de tomar

una máscara de cera sobre un cadáver poder exhibirlo en el atrio de las casas y se llevaran en público en los cortejos fúnebres; sólo tenían éste derecho las familias nobles. Claro que éste es el punto de partida pero se refiere a la imagen en su aspecto material, y no en el concepto de imagen al que queremos llegar, como un signo de identidad, de individualidad, como una manifestación esencial de la personalidad, ya que constituye uno de los elementos fundamentales de la proyección externa de la persona.

Ana Azurmendi Adarraga divide en tres períodos el recorrido del derecho a la propia imagen hasta su reconocimiento como derecho humano.

1. 1839 a 1900. Es la etapa en que comienza a reconocerse el derecho a la imagen, pero considerado como un aspecto particular del derecho de autor.

Así está contenido este derecho en tal sentido en las leyes sobre propiedad intelectual y artística de Alemania (1876), Austria (1885) y Bélgica (1886), que constituyen el primer paso hacia la regulación del mismo; sin embargo, podemos decir que en este período no hay aún conciencia jurídica de la existencia de un derecho a la propia imagen. La jurisprudencia francesa reconoce de manera implícita en la segunda mitad del siglo XIX el derecho a la propia imagen, por supuesto, con contornos confusos y sobre todo en cuanto a la relación de este derecho con la entonces llamada libertad de prensa, y obviamente que aún no se vislumbraba la aparición de la informática y la incidencia que tendría en el desarrollo del contenido del derecho a la imagen.

2. 1900 a 1919. Con el cambio de siglo se produce un cambio de la perspectiva en la concepción jurídica en el derecho a la propia imagen, tanto desde la jurisprudencia como la doctrina comienza a ser tratado como un bien esencial de la persona. Es decisiva la influencia que tienen en este período, a) Por un lado, en el ámbito europeo, sobre todo en Francia y en Italia la doctrina alemana de los derechos de la personalidad. Gierke es uno de los doctrinarios, que si bien no trata específicamente la imagen humana su obra permite el marco jurídico adecuado para hacer que el derecho a la imagen se vaya desvinculando de los derechos de autor. Esto parte de conceptos tales como expone en su trabajo, el derecho general de la personalidad tiene por objeto esencial el libre desarrollo de su propia personalidad. Si Gierke va a proporcionar resortes doctrinales válidos para el reconocimiento de la naturaleza jurídica de la imagen humana, no es menos cierto que su teoría dará pie a que bajo la noción del libre desarrollo de la personalidad se comiencen a desdibujar las fronteras entre honor, intimidad e imagen de la persona. En 1902 en el marco del XXVI Congreso de Juristas Alemanes, celebrado en Berlín, queda abiertamente reconocido el derecho a la propia imagen como uno de los derechos inherentes a la personalidad. b) Por otro lado, hacia fines del siglo pasado en Estados Unidos se conocía el célebre artículo de Warren y Brandeis "The right of privacy" de 1890, que se refiere al derecho a la imagen personal como la forma más simple del *right of privacy*, y cuyo antecedente más inmediato es la expresión acuñada por el juez Cooley en 1879, *the right to be let alone*, "el derecho a ser dejado en paz". Estos autores plantean que si la *Common Law* cada vez ampliaba más su protección a las personas y a sus bienes, dicha protección debía extenderse a los particulares en su vida privada y si se tenían en cuenta las nuevas circunstancias sociales, tecnología y desarrollo de la prensa, crecimiento del interés informativo, etc., sería conveniente considerar al *right of privacy* como reconocido por la cuarta enmienda de la Constitución Americana. En 1904, por primera vez, un Tribunal Supremo, el de Georgia en el caso "Pavesich vs. New England Life Insurance Co." sanciona la utilización publicitaria del rostro de una persona sin su consentimiento; y en 1909 el Tribunal Supremo de Kentucky dicta una sentencia en igual sentido. Queda así ratificado el doble contenido del *right of privacy*, la defensa de la vida privada del individuo y la de evitar el uso de la propia imagen sin consentimiento de la persona representada.

3. 1910 a 1948. Es el período llamado de consolidación del derecho a la propia imagen en el que se orienta definitivamente el derecho hacia un nuevo marco jurídico: el de los derechos humanos. Con las características propias de los planteos jurídicos de cada país, este derecho tiene sus primeras manifestaciones en las peticiones de reconocimientos constitucionales y en la consolidación de los derechos de la personalidad como el marco ideal para la comprensión del derecho a la propia imagen.

En 1928, en el caso "Olmstead vs. United States", el Tribunal decidió no reconocer el *right of privacy* implícito dentro de la cuarta enmienda; tuvieron que pasar treinta años para que fuera así reconocido por el mismo tribunal. En la doctrina mientras se abría el camino en el sentido de que el derecho a la propia imagen, como elemento del *right of privacy* se consideraba "uno de los derechos más valiosos de los ciudadanos", se estaba preparando el terreno para su reconocimiento como un derecho humano. En Estados Unidos no rige un reconocimiento positivo del carácter federal del derecho a la propia imagen, pero sí es de destacar que cada vez hay más normas que tutelan algunos de sus aspectos y la tendencia a un reconocimiento constitucional del *right of privacy*. Finalmente, en 1965 el Tribunal Supremo Federal decidió, en el caso "Griswold Connecticut", que el *right of privacy* está implícitamente reconocido por la Constitución de los Estados Unidos en la cuarta enmienda.

4. Nosotros situamos la cuarta etapa a partir de 1948, con la declaración Universal de Derechos del Hombre, que si bien no obliga a los Estados, su influencia es notoria en los textos constitucionales posteriores a ella.

En lo que respecta a los derechos tutelados; es el primer artículo de la ley, al describir el objeto de la misma que establece:

Es necesario mencionar que en los textos supranacionales no se menciona el derecho a la propia imagen expresamente, pero surge implícitamente de muchos de ellos. En la Declaración Universal de 1948 el artículo 12 se refiere a la vida privada y a la honra; asimismo el artículo 30 expresa «Nada de la presente declaración podrá interpretarse en el sentido de que confiere derecho alguno al Estado, a un grupo o a una persona, para emprender y desarrollar actividades o realizar actos tendientes a la supresión de cualquiera de los derechos y libertades proclamados en esta declaración». En el Pacto Internacional de Derechos Económicos, Sociales y Culturales de 1966 en el artículo 19.1. «...Nadie podrá ser molestado en sus opiniones... a) Asegurar el respeto a los derechos o a la reputación de los demás; y el artículo 5 es casi exacto al 30 de la Declaración Universal. En Argentina rigen estas normas después de la reforma de 1994, quedando incorporadas a nuestra Constitución por el artículo 75. Inciso 22.

Los textos constitucionales que tienen expresamente incorporadas normas en las que se reconoce el derecho a la propia imagen son:

1. La Constitución Portuguesa de 1976; artículo 26; 1- «Todos tendrán derecho a la intimidad personal, a la capacidad civil, a la ciudadanía, al buen nombre y a la reputación, a la imagen y a la intimidad en su vida privada»
2. La Constitución Peruana de 1993 artículo 2 «Toda persona tiene derecho ... 5. Al honor y a la buena reputación, a la intimidad personal y familiar y a la propia imagen»
3. La Constitución Brasileña de 1988 artículo 5 «Se garantiza el derecho...V.de réplica, proporcional al agravio, y a la indemnización por daño material, moral o a la imagen».
4. La Constitución Española de 1978 artículo 18 «se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen»; artículo 20.1 «se reconocen y protegen los derechos: d) a comunicar y recibir libremente información veraz por cualquier medio de difusión... 4- Estas libertades tienen un límite en el respeto de los derechos reconocidos en este título, en los preceptos especialmente en el derecho al honor, a la intimidad personal y familiar, a la propia imagen...». Queda claramente establecido el límite entre el derecho de dar y recibir información y el derecho a la imagen como parte del derecho a la privacidad. Además rige la Ley Orgánica 1/1982 en la que se establece como lesivo al derecho de la personalidad, artículo 7, 3. «la divulgación de hechos relativos a la vida privada de una persona o familia que afecten a su reputación o buen nombre...». 4. «la revelación de datos privados de una persona o familia conocidos a través de la actividad profesional u oficial de quien los revela».

En los textos constitucionales prerreferidos que mencionan específicamente el derecho a la imagen propia y la herramienta o garantía de protección de ese derecho es el *hábeas data*.

En nuestra Ley fundamental no hay un artículo que se refiera al derecho a la imagen propia, o al propio perfil, pero está implícito a través de las normas supranacionales que quedaron incorporadas a nuestra Constitución después de la reforma de 1994, en el artículo 75, inciso 22. Por su parte, el artículo 43 establece la garantía de *hábeas data* como el acceso a los datos, y la finalidad que se dará a los mismos y la posibilidad según los casos de rectificación, supresión, confidencialidad y actualización de los mismos. Nada dice en relación a los derechos protegidos en doctrina varios autores consideran entre los derechos tutelados por esta garantía el derecho a la propia imagen.

Vemos que al referirse a los bienes jurídicos tutelados «de nada sirve que llenemos los anaqueles con dispositivos legales que protejan otros aspectos como los bienes u otros desenvolvimientos de esa misma persona, si no empezamos por proteger lo más inherente a esa propia persona, que es el derecho a su perfil y el derecho a su imagen» En ese sentido también enumeran el derecho a la imagen como bien jurídico tutelado por el *hábeas data* Merovich; Puccinelli; Santos Cifuentes también reconoce entre los derechos personalísimos de las personas a amparar a través del instituto tales como honor, buena reputación, intimidad, identidad, imagen y voz.

Toda persona que vive en una sociedad tecnológicamente desarrollada, a diario brinda información sobre sus datos personales: domicilio, número de teléfono, documento de identidad, profesión, estado civil, miembros que integran su familia, participación académica o gremial, militancia en partidos políticos, creencias religiosas, estudios cursados, desempeño laboral, si posee o no tarjetas de créditos, cuenta bancaria o automóvil, etc.; todo ello susceptible de ser almacenado en banco de datos o archivos, si se entrecruza esa información se obtiene un perfil total de la persona, una verdadera radiografía, la imagen en su totalidad, creemos que sin dudas está tutelado por medio de esta garantía el derecho a la imagen propia y al perfil propio, que va a depender en muchos casos de la utilización que se dé a los datos personales. A través de la protección de la imagen propia una persona tiene la posibilidad de proteger su buen nombre, su honor, su honra, su buena reputación y su dignidad, todos ellos conceptos que quedan comprendidos dentro del concepto de derecho a la propia imagen.

«Artículo 1° (Objeto). La presente ley tiene por objeto 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, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional».

En este punto objetamos la ley por considerar, como lo hemos expuesto, que esta garantía constitucional no se circunscribe únicamente a la protección de la intimidad y el honor, sino que abarca una amplia gama de derechos en lo que son contestes la doctrina y la jurisprudencia. En esto la ley es acotada, y no tomó en cuenta los mencionados *standard* de protección.

V. JURISPRUDENCIA

Antes de la sanción de la Ley 25.326; de protección de datos personales y *habeas data*, la jurisprudencia es la que ha ido delineando los contornos de esta nueva garantía constitucional.

Dentro de este marco aparecen como especialmente importantes los fallos de la Corte Suprema en el tema; *Facundo Raúl Urteaga*³⁰, de noviembre de 1998; y *Ganora, Mario Fernando y otros*, del 16 de septiembre pasado de 1999.

V.1 Urteaga, Facundo

Éste promueve ante la justicia federal en lo contencioso administrativo una acción con sustento en el artículo 43 de la Constitución contra el Estado nacional (Fuerzas Armadas y órganos de información e inteligencia) y contra la Provincia de Buenos Aires para obtener la información sobre su hermano Benito Jorge Urteaga supuestamente “abatido” en un enfrentamiento en Villa Martelli, en 1976. La Cámara rechaza la acción intentada con fundamento en a) la falta de legitimación del actor y b) la improcedencia de la vía procesal elegida; considerando que la vía correcta es la del *habeas corpus*.

Sin embargo, la Corte hace lugar al recurso extraordinario y dicta un fallo de gran valor para la interpretación de esta nueva garantía constitucional; del mismo que personalmente considero en un futuro hablaremos como un *leading case*.

- a. Sobre el primer planteamiento, o sea, la falta de legitimidad, la Corte establece que conviene recordar una vieja doctrina según la cual la falta de reglamentación no debe obstaculizar la vigencia de ciertos derechos, y que

30. Publicado en *La Ley* 25/11/98.

las garantías individuales protegen a los individuos por el solo hecho de estar consagradas en la Constitución, independientemente de las leyes reglamentarias; de manera tal, que la ausencia de las mismas no es óbice para su ejercicio; y que dentro del marco constitucional no reglamentado aún por el órgano competente, corresponde a la Corte delinear los alcances de la garantía mencionada con razonable flexibilidad; Cabe en este caso la frase de la Corte americana en el fallo *Mc Culloch vs. Maryland*³¹, cuando dice *no nos olvidemos que lo que estamos interpretando es una constitución*; esta flexibilidad de la Corte en su interpretación que ha sido fundamental en lo relacionado con la legitimación del actor, puesto que si se hubiera limitado a hacer una interpretación literal, el artículo 43 de la Constitución Nacional se refiere a *toda persona podrá tomar conocimiento de los datos a ella referidos*, y en este fallo queda establecido que también procede esta acción para tomar conocimientos de los datos de otras personas cuando tengamos la calidad de "afectado"; o sea, cuando nos concierne directamente³².

Esta postura ha sido sostenida por la doctrina mayoritaria³³ (Ekmekdjian y Pizzolo, Puccinelli, Falcón siguiendo a Santos Cifuentes se refieren a la línea sucesoria del artículo 3592 del C.C.); también por otros tribunales, como la Cámara Primera de Apelaciones en lo contencioso administrativo de Córdoba, en el caso García Llanos en 1995, que afirma con un criterio amplio que toda persona física o jurídica interesada, a quien el dato concreto afecte un derecho subjetivo o tenga un interés legítimo tiene legitimación activa para interponer acción de *hábeas data*. En este sentido, la Constitución de la Provincia de Buenos Aires es clara al admitir, en su artículo 20, la posibilidad de acceso a los datos a los *terceros con interés legítimo*.

Es importante mencionar en este punto que la "Ley de Protección de Datos Personales" no se aparta de la postura "aperturista" en relación con la legitimación, de nuestro máximo Tribunal; así lo establece el

Artículo 34. (Legitimación activa). «La acción de protección de los datos personales o de *hábeas data* podrá ser ejercida por el afectado, sus tutores o curadores y los sucesores de las personas físicas, sean en línea directa o colateral hasta el segundo grado, por sí o por intermedio de apoderado. Cuando la acción sea ejercida por personas de existencia ideal, deberá ser interpuesta por sus representantes legales, o apoderados que éstas designen al efecto. En el proceso podrá intervenir en forma coadyuvante el Defensor del Pueblo».

31. *Mc Culloch vs. Maryland*, 17 U.S.316 (1819).

32. BIANCHI, Alberto B. "El *hábeas data* como medio de protección del derecho a la información objetiva en un valioso fallo de la Corte Suprema". *La Ley*, Suplemento de Derecho Administrativo, 27 de noviembre de 1998, pp. 1-6.

33. DALLA VÍA-BASTERRA, *op. cit.*, pp. 127-129.

- b. Respecto al segundo planteo; o sea que la vía elegida debió ser una acción de *hábeas corpus*; criterio que no compartimos, puesto que han transcurrido 22 años desde la desaparición del hermano de quien interpone la acción, y tal como lo explica el ministro Petracchi en su voto, *el objeto específico de la acción intentada es la obtención de datos y por lo tanto sólo resulta viable mediante el hábeas data*³⁴.

Con base en lo establecido en la Constitución Nacional, la jurisprudencia de Tribunales Inferiores I ha acogido tempranamente esta acción como una forma de amparo, tal lo dispuesto por la Cámara Nacional de Apelaciones en lo Civil, en autos *Rossetti c/ Dun Bradstreet S.R.L. s/Amparo*³⁵ *...cuando a través del amparo, un particular ejerce la acción de hábeas data...*

En este caso la Corte tiene dos votos minoritarios en los cuales se interpreta, en uno de ellos (Belluscio y López), que la acción que procede en este caso es una acción de amparo; en otro de los votos minoritarios (Fayt y Bossert), que la acción correspondiente en este caso es el *hábeas data* como una especie de amparo. Sin embargo, el voto de la mayoría, formada por los ministros Nazareno, Moliné O'Connor, Petracchi, Boggiano y Vázquez, entendió que la acción correcta era la de *hábeas data*. Pero, estas dudas quedan subsanadas por la nueva ley; surgiendo claramente como lo explicáramos del juego de los artículos 33 y 37.

V.2 El derecho a la verdad: creación pretoriana

El fallo si bien está compuesto por siete votos diferentes, todos coinciden en la solución final y en la naturaleza del derecho protegido; lo que consideramos la nota más sobresaliente del fallo; en este caso el derecho protegido es *el derecho a la verdad objetiva*, y más allá del *nomen iuris* que el actor le haya dado a la acción y de la vía procesal que técnicamente corresponda debe hacerse efectivo. Esto constituye una verdadera novedad puesto que no hay otro precedente en el mundo de la tutela del *hábeas data* al derecho a la "verdad objetiva", como parte del derecho a la privacidad, porque los derechos tutelados tradicionalmente por esta garantía son el derecho a la intimidad, al honor, a la dignidad y a la propia imagen.

Fayt consideró que los derechos humanos en juego, en este caso, requieren de la garantía del derecho a la información para posibilitar el impostergable cumplimiento de la ética de la verdad³⁶.

34. Considerando 7°.

35. C.N.A.C., sentencia del 19/5/1995.

36. Considerando 13°.

Según Bidart Campos³⁷, a partir de la causa *Suárez Mason*³⁸, se introducen dos cuestiones en relación con el tema; la primera es, si en relación con las personas desaparecidas entre 1975 y 1983, existe un "derecho" de sus familiares a conocer la "verdad objetiva" sobre los acontecimientos ocurridos; lo que implicaría un derecho de esos familiares a conocer los "datos existentes"; y la segunda es si ese derecho es amparado por la innominada garantía de *hábeas data*.

Además agrega: *¿Cuál es la notoria diferencia que se acusa respecto del derecho a la verdad y a los datos acerca de víctimas desaparecidas?*; concluyendo que cuando se trata de este tipo de casos; lejos de querer ocultar o mantener reserva sobre los datos de una persona, lo que se pretende, en contrario, es que se informe y se sepa públicamente lo que en verdad ocurrió con la víctima desaparecida. La "verdad" y los "datos" a los que se pretende acceder no habrán de reservarse, sino –a la inversa– descubrirse y darse a publicidad (considerando 8° doctor Fayt).

Lo que finalmente se pregunta Bidart Campos es si en realidad esa diferencia hace que no corresponda que sea la clásica acción de *hábeas data*, una de las vías procesales posibles mediante la cual requerir los datos de la víctima desaparecida para saber lo que realmente ocurrió.

Obviamente contesta por la negativa; postura a la que adherimos; el hecho de que el *hábeas data* haya nacido con el fin de preservar la intimidad informativa no significa que allí queda agotado su funcionamiento:

«Toda garantía constitucional debe ser tan elástica cuanto la realidad de una situación determinada lo demande; y ello a efectos de que rinda su efecto tutelar respecto del derecho que a través de esa misma garantía se pretende. Las garantías deben holgarse y si, acaso, nunca antes nos imaginamos que íbamos a precisar alegar un "derecho" a la verdad... ahora que se hizo necesario hay que buscar con aperturismo y activismo procesal y judicial la mejor vía conducente, en cada caso, para que haya una, o más, garantías a disposición de quien invoca aquel derecho. Si las garantías no sirven para el fin por el cual existen, no sirven para nada»³⁹.

Juan Mendez⁴⁰ explica que el "derecho a la verdad", en el Derecho Internacional de los Derechos Humanos, es un "principio emergente". Ello es así porque no estamos ante una norma explícita de los tratados y, por lo tanto, de vigencia incuestionable. El hecho de que tenga el carácter de "principios

37. BIDART CAMPOS, Germán J., *¿Hábeas data, o qué? ¿Derecho a la verdad o qué?*, *La Ley*, 15 de febrero de 1999, p. 27.

38. "Suárez Mason, Carlos G. S. Homicidio, privación ilegal de la libertad, etc." Causa S.1085.XXXI, resuelta el 13 de agosto de 1998.

39. BIDART CAMPOS, *op. cit.* p. 24

40. MENDEZ, Juan E., *Derecho a la verdad frente a las grandes violaciones de los derechos humanos*, Ed. Del Puerto, Argentina, 1997, p. 517; citado por GIL DOMÍNGUEZ, Andrés, "La verdad: un derecho emergente", *La Ley "Suplemento de Derecho Constitucional"*, 15 de febrero de 1999, pp. 28-29.

emergentes" y no de normas convencionales, claras como normas vinculantes: por tratarse de la interpretación de buena fe de normas obligatorias, tendrían la misma eficacia. En este contexto, el derecho a la verdad genera la obligación del Estado de investigar y dar a conocer los hechos que se puedan establecer fehacientemente.

Gil Domínguez⁴¹ opina que el derecho a la verdad integra el *bloque de constitucionalidad federal*, y desde la cúspide normativa infiltra al derecho infraconstitucional. En el caso *Urteaga*, el derecho a la verdad creado por vía pretoriana reafirma el derecho de toda persona y su familiares de saber la verdad acerca de las víctimas de la desaparición forzada de personas.

V.3 El secreto de Estado. Límites

Es necesario destacar que en el fallo *Urteaga* se consagra en forma unánime un principio importante, que es la obligación del Estado de producir información objetiva sobre los datos que posea en sus bancos o registros. Obviamente como todo principio, éste tendrá sus excepciones que no están indicadas en el fallo porque será materia del Congreso establecerlas; pero en nuestro país donde no existe una ley equivalente a la *Federal Information Act de los Estados Unidos* es muy valioso este reconocimiento por parte de la Corte Suprema⁴²; principio que sostiene y reafirma en el fallo de 16 de septiembre pasado en el fallo *Ganora Fernando y otra s/ hábeas corpus*⁴³.

Los doctores Mario Fernando Ganora y Rosalía Liliana Magrini, quienes habían sido patrocinantes del señor Adolfo Silingo en varias causas, interpusieron acción de *hábeas corpus* con fundamento en que personas desconocidas habían realizado indagaciones acerca de las actividades por ellos realizadas. Al respecto alegan que

«ante la posibilidad cierta de que se estuvieran realizando investigaciones o actividades de inteligencia respecto de nuestras personas que entrañan una verdadera perturbación de la intimidad, tranquilidad y seguridad en el ejercicio profesional reclamamos saber qué autoridad y con qué propósito las ha ordenado, a los efectos de prevenir e impedir que sin orden de autoridad judicial competente pudiera verse amenazada nuestra libertad ambulatoria o el derecho a no ser objeto de injerencias arbitrarias o abusivas en nuestra vida privada...».

En la misma presentación interponen acción de *hábeas data* a los efectos de

«tomar conciencia de los datos que existen sobre nosotros en los registros policiales y de la fuerza de seguridad y organismos de inteligencia para que en caso de

41. GIL DOMÍNGUEZ, *op. cit.*, p. 32.

42. BIANCHI, Alberto B., *op. cit.*, p. 2.

43. Sentencia de la Corte Suprema de Justicia de la Nación G. 529. XXXIII.

falsedad o discriminación se exija judicialmente la supresión, rectificación o actualización de los mismos⁴⁴.

Tanto el juez de primera instancia como la Cámara Nacional de Apelaciones en lo Criminal y Correccional no hicieron lugar a las peticiones de los actores; en relación con el *hábeas corpus* sobre la base de que no existiría una amenaza o limitación actual de la libertad ambulatoria; y en relación con la acción de *hábeas data* por considerar que

«la información que se pide debe ser pública o al alcance de los particulares. La obrante en las fuerzas y organismos de seguridad no reviste tal carácter por obvias razones de seguridad pública»⁴⁵.

En consecuencia, contra tal decisión dedujeron los mismos y el Colegio Público de Abogados recurso extraordinario el que fue concedido en ambos casos.

En todos los votos se establece que la impugnación del Colegio Público de Abogados fue mal concedida, y que no está habilitado para interponer el remedio federal previsto en el artículo 14 de la Ley 48, por no ser parte en el proceso, aunque invoque un gravamen como consecuencia de dicha decisión. Asimismo, de todos los votos surge que corresponde declarar admisible el recurso interpuesto por los doctores Ganora y Magrini.

El meollo de la cuestión consiste en decidir si la obtención de información sobre datos personales obrantes en los registros de las Fuerzas Armadas y organismos de seguridad se halla amparada por la norma del artículo 43 de la Constitución Nacional; y si es así cuáles son los límites.

En la mayoría de las constituciones se han establecido limitaciones al acceso de datos, basados fundamentalmente en razones de seguridad de los respectivos Estados; por ejemplo, Brasil (1988); Perú (1993); España (1978); así también en la *Freedom of Information Act*. En nuestra Constitución no está establecido específicamente, sino simplemente el artículo 43 prevé el acceso a los bancos de datos públicos, sin establecer excepciones. Pero como bien lo han fundamentado los convencionales constituyentes, entre ellos el convencional Delich que explicó

«a mucha gente le molesta el secreto de Estado y con razón; puesto que en tanto más amplia es la zona de secreto, más reducida es la zona de transparencia ligada a la construcción de la democracia en la sociedad. De modo que nadie podría hacer el elogio de la necesidad indefinida del secreto de Estado, pero también es cierto que nadie podría imaginar un Estado que no es capaz de proteger

44. Considerando 2°.

45. Considerando 3°.

y guardar esa zona oscura..., entonces la única solución que tenemos –y es la que vamos a instrumentar– no es pensar ni imaginar un Estado carente de secreto. Lo que sí vamos es a posibilitar que ese secreto no sea para siempre, que sea acotado... Tiene que haber un momento en el cual este secreto se decida racionalmente, y otro en el cual sea levantado, entonces no desprotegemos al Estado pero tampoco a la sociedad; no dejamos al Estado sin una herramienta decisiva pero tampoco posibilitamos que un ciudadano esté indefenso frente a los secretos del Estado».

En el fallo Ganora, la Corte ha sido consecuente con este lineamiento, puesto que resuelve que la obtención de información sobre datos personales obrantes en los organismos y fuerzas de seguridad halla adecuación legal en la acción de *habeas data*; ello sin perjuicio de que el suministro de esa información pueda eventualmente afectar la seguridad, la defensa nacional y las relaciones exteriores, situación que deberá ser invocada por el titular de la respectiva institución en cada caso concreto. La decisión de la Cámara de rechazar la acción, por considerar que los particulares no pueden tener acceso a la información obrante en las Fuerzas Armadas y organismos de seguridad, constituye una afirmación dogmática carente de razonabilidad. Porque no se han librado los oficios correspondientes no ha habido respuesta por parte del titular de la institución explicando si existen razones para impedir al legitimado el acceso a las mismas. De manera tal que los datos obrantes en las fuerzas de seguridad, incluso los reservados y con carácter secreto están especialmente contenidos en la norma del artículo 43 de la Constitución Nacional.

Creo que la importancia de estos fallos reside en que nos permite afirmar, sin temor a equivocarnos, que estamos ante una saludable reafirmación de esta nueva garantía constitucional; siguiendo la línea trazada por los constituyentes del 94; por la jurisprudencia de tribunales inferiores y por la doctrina. Se van delimitando de esta forma los contornos de la figura acorde también con el ámbito internacional.

Por ello hemos reiterado en alguna oportunidad⁴⁶.

«que las decisiones de la Corte en ambos casos, lejos de ser válidas hasta tanto se sancione una ley reglamentaria, es ésta la que deberá sancionarse teniendo en cuenta expresamente lo establecido desde nuestro más Alto Tribunal; que con un criterio garantista; 1) amplía la legitimación del artículo 43 de nuestra Constitución Nacional; extendiéndola a los familiares de las víctimas; 2) crea un nuevo derecho; el "derecho a la verdad"; 3) establece en todos que en todos los casos en que esté comprometido el secreto de Estado, el mismo, será acotado a un determinado tiempo, debiendo existir fundamentación por parte de la autoridad que corresponda. Si las garantías no sirven para el fin con que fueron creadas; no sirven de nada».

46. BASTERRA, Marcela, "Los derechos tutelados por el *habeas data*. Doctrina y Jurisprudencia". Capítulo perteneciente a la obra colectiva *Habeas data*, coordinada por GOZALINI, Osvaldo, Ediar.

La nueva ley toma estos principios regulando el manejo de los archivos o registros de Seguridad del Estado, en los artículos 17, 18 y 23 de la siguiente manera:

«**Artículo 17** (Excepciones). 1. Los responsables o usuarios de bancos de datos públicos pueden, mediante decisión fundada, denegar el acceso, rectificación o la supresión en función de la protección de la defensa de la Nación, del orden y la seguridad públicos, o de la protección de los derechos e intereses de terceros. 2. La información sobre datos personales también puede ser denegada por los responsables o usuarios de bancos de datos públicos, cuando de tal modo se pudieran obstaculizar actuaciones judiciales o administrativas en curso vinculadas a la investigación sobre el cumplimiento de obligaciones tributarias o previsionales, el desarrollo de funciones de control de la salud y del medio ambiente, la investigación de delitos penales y la verificación de infracciones administrativas. *La resolución que así lo disponga debe ser fundada y notificada al afectado.* 3. Sin perjuicio de lo establecido en los incisos anteriores, se deberá brindar acceso a los registros en cuestión en la oportunidad en que el afectado tenga que ejercer su derecho de defensa».

Artículo 18 (Comisiones legislativas). Las Comisiones de Defensa Nacional y la Comisión Bicameral de Fiscalización de los Órganos y Actividades de Seguridad Interior e Inteligencia del Congreso de la Nación y la Comisión de Seguridad Interior de la Cámara de Diputados de la Nación, o las que las sustituyan, *tendrán acceso a los archivos o bancos de datos referidos en el artículo 23 inciso 2 por razones fundadas y en aquellos aspectos que constituyan materia de competencia de tales Comisiones.*

Artículo 23 (Supuestos especiales). 1. Quedarán sujetos al régimen de la presente ley, los datos personales que por haberse almacenado para fines administrativos, deban ser objeto de registro permanente en los bancos de datos de las fuerzas armadas, fuerzas de seguridad, organismos policiales o de inteligencia; y aquellos sobre antecedentes personales que proporcionen dichos bancos de datos a las autoridades administrativas o judiciales que los requieran en virtud de disposiciones legales. 2. *El tratamiento de datos personales con fines de defensa nacional o seguridad pública por parte de las Fuerzas Armadas, fuerzas de seguridad, organismos policiales o inteligencia, sin consentimiento de los afectados, queda limitado a aquellos supuestos y categoría de datos que resulten necesarios para el estricto cumplimiento de las misiones legalmente asignadas a aquéllos para la defensa nacional, la seguridad pública o para la represión de los delitos. Los archivos, en tales casos, deberán ser específicos y establecidos al efecto, debiendo clasificarse por categorías, en función de su grado de fiabilidad.* 3. Los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento⁴⁷.

Es difícil determinar qué ocurre con el acceso a los registros de los organismos de inteligencia del Estado, especialmente si tenemos en cuenta la importancia y necesidad de confidencialidad de determinada información en relación con los temas concernientes a la seguridad nacional, pero es menester tener presente que el constituyente tuvo claramente la intención de

establecer a través del *hábeas data* una protección a los ciudadanos, precisamente en muchos casos frente a esos registros. Consideramos que la ley al establecer en qué casos; bajo qué condiciones o circunstancias se va a mantener el secreto del Estado en relación con los datos personales, ha logrado el equilibrio que surge como una necesidad desde la Constitución, la jurisprudencia y la doctrina, casi por unanimidad

VI. SECRETO DE LAS FUENTES DE INFORMACIÓN PERIODÍSTICAS

El artículo 43 de la Constitución Nacional establece en el tercer párrafo *in fine* «...no podrá afectarse el secreto de las fuentes de información periodística», un viejo reclamo que fue recogido en esta expresión a propuesta del convencional constituyente Antonio M. Hernández⁴⁸.

Parte de la doctrina sin embargo considera que no es la única fuente exceptuada de afectación, puesto que si bien ésta es la única mencionada expresamente por el articulado de la Constitución, podría incluirse entre las fuentes exceptuadas la que se refiere a la seguridad de Estado y secreto profesional. Bazán nos dice que la limitación en realidad es “el secreto de la fuente” con lo que debió extenderse la inmunidad hacia otros sectores alcanzados por el secreto, siguiendo a Quiroga Lavié cuando afirma:

«no sólo las fuentes periodísticas merecen dicha protección sino todas las otras actividades profesionales implicadas por el secreto: el servicio de los médicos, de los sacerdotes, de los abogados y demás actividades que, obligados a recibir informes reservados o secretos, debieran, del mismo modo que los periodistas, encontrarse amparados por una protección constitucional equivalente»⁴⁹.

Creemos que al sancionarse la ley de *hábeas data* en relación con este tema, se tuvo especial cuidado de no desvirtuar las miras que tuvo el constituyente al dictar la norma, de la que surge, sin lugar a dudas, una interpretación fiel de que la misma es una garantía para proteger especialmente a los individuos, y no especialmente a los bancos de datos, que como ya se ha dicho son objeto de tutela de otros derechos constitucionales, tal como el de trabajar, comerciar, ejercer toda industria lícita, etc. Y si interpretamos la expresión de la “protección a las fuentes de información periodística”, creemos que se ha querido equilibrar y proteger especialmente la libertad de prensa.

Es importante destacar que antes de la reforma de la Constitución de 1994, había proyectos, tanto en la Cámara de Diputados como en la de Senadores,

48. DALLA VÍA, Alberto Ricardo, *Constitución de la Nación Argentina*. Texto según la reforma de 1994, Librería Editora Platense, noviembre 1994, p. 28.

49. BAZÁN, Víctor, “El *hábeas data* después de la Reforma Constitucional”, *Boletín Asociación Argentina de Derecho Constitucional*, agosto 1995, n. 112, p. 7.

que establecen el secreto de las fuentes de información; así también normas en nuestro derecho público provincial y en el derecho comparado. Era la oportunidad esperada de poder introducir este párrafo en el artículo 43 de la Constitución Nacional. Así lo explica el convencional Hernández en la 18ª reunión de Comisión de Redacción, 1/8/94.

«Es de gran importancia destacar el papel protagonista que tiene en la sociedad moderna la libertad de prensa; basta con mencionar a modo de ejemplo el voto del Juez de la Corte Suprema de Justicia de la Nación doctor Fayt en el caso "Verbitsky" donde queda establecido claramente que prevalece el derecho de quien recibe información por sobre el derecho de quien la emite, el objeto del sistema es preservar la información. En el voto en disidencia del juez Fayt donde recuerda que el fundamento de la interdicción de la censura es precisamente asegurar un libre acceso a la información. "La prensa tiene una situación estratégica en la sociedad contemporánea. Saber qué pasa, estar informado, acceder a la verdad objetiva constituyen reclamos de nuestro tiempo. La información condiciona la existencia y las actividades de cada sociedad y la participación resulta imposible sin ella"⁵⁰.

Es indudable que la libertad de expresión fuertemente protegida en nuestra Carta Magna y a través de la abonada jurisprudencia resultante de la interpretación de los artículos 14 y 32 de la Constitución Nacional, una vez más sale fortificada en la redacción del artículo 43. Compartimos la intención del constituyente de buscar un equilibrio razonable que no vulnere la libertad de prensa, esto además porque en un sistema garantista como el nuestro y acorde con los principios de un Estado Democrático de Derecho el ejercicio de ningún derecho puede resultar en detrimento del ejercicio de otro; de manera que ninguna ley hubiera sido constitucional si hubiera alterado este privilegio en favor de la libertad de expresión establecido expresamente en nuestra constitución.

Se trata de impedir a través de esta disposición la virtual autocensura de todos aquéllos que tuvieren informaciones útiles a la función de información e investigación que debe cumplir la prensa, por temor a encontrarse incluidos en algún tipo de responsabilidad sea civil o penal, o de ser objeto de represalias como consecuencia de haber facilitado los datos que luego la prensa hace públicos. Sin una cláusula garantizadora del secreto de las fuentes de información periodística, el ejercicio de la libertad de prensa podría convertirse de hecho en ilusorio⁵¹.

En este sentido Vanossi explica que en ningún caso el *hábeas data* debe ser utilizado como un modo de censura previa así como tampoco para borrar datos obrantes en esos archivos. Por ello el constituyente utilizó la expresión

50. Fallo C.S. junio 13, 1989, *La Ley*, 1989-D, p. 183.

51. QUIROGA LAVIÉ, Humberto, *op. cit.*, p. 160.

“no podrá afectarse el secreto de las fuentes de información periodística”⁵². Concordantemente con esto Puccinelli considera que la norma constitucional tiende a proteger la identidad del informante para obtener un *bill* de indemnidad a efectos de acumular la información de quien fuese y como se quisiese, lo que resultaría de gran utilidad para llevar a cabo las campañas discriminatorias que pretende prevenir el texto constitucional⁵³. Sin embargo, Vázquez Ferreyra dice que la justificación del secreto del periodista no está precisamente en la protección de la intimidad del informante, ni en el deber de sigilo ante una relación de confianza, sino en el derecho a la información en el que por tratarse de un interés colectivo el titular de la información es la sociedad, y el intermediario es el periodista. La protección del periodista, en tanto desee guardar secreto sobre la fuente de información, es una necesidad propia de nuestros tiempos y una herramienta de la lucha contra la corrupción⁵⁴.

Es necesario aclarar que al referirse a la afectación de la “fuente” no significa por ello que no podamos conocer los datos que acerca de nosotros posea un banco o registro determinados, sino que lo que no va a poder conocerse es el origen de esa información.

En la Constitución de la Ciudad Autónoma de Buenos Aires, en su artículo 16, el constituyente ha querido salvaguardar también el secreto de la fuente de información periodística, al igual que los constituyentes nacionales en la reforma de 1994.

No ocurre lo mismo con la Constitución de la Provincia de Buenos Aires que establece:

«no podrá afectarse el secreto de las fuentes y el contenido de la información periodística»

con lo que el límite se amplía y abarca no sólo las fuentes, sino que al referirse a los contenidos no podría afectarse, por ejemplo, la veracidad de una información periodística:

«con lo cual se avizora el peligro de caer en la dictadura de los medios de comunicación»⁵⁵.

La Ley 25.326 aclara estas dudas, ya desde su **artículo 1º**, al establecer...

52. VANOSI, Jorge Reinaldo, *op. cit.*, p. 948.

53. PUCCINELLI, Oscar Raúl, “*Hábeas data*: aportes para una eventual reglamentación”. Ed.17/2/95

54. VÁZQUEZ FERREYRA, Roberto, “El derecho a la información y el secreto profesional de los periodistas”, J.A. 1991-IV-619/622.

55. GALLARDO, Cecilia, OLMEDO, Karina y FLORI, José Luis, “¿Cuáles son los límites del hábeas data? *La Ley* 1997-3 p. 644

«En ningún caso se podrán afectar la base de datos ni las fuentes de información periodísticas».

En relación con el secreto de otras fuentes, tal el caso del "secreto profesional", lo contempla especialmente en el

«**Artículo 10** (Deber de confidencialidad). 1. El responsable y las personas que intervengan en cualquier fase del tratamiento de datos personales están obligados al secreto profesional respecto de los mismos. Tal obligación subsistirá aun después de finalizada su relación con el titular del archivo de datos. 2. El obligado podrá ser relevado del deber de secreto por resolución judicial y cuando medien razones fundadas relativas a la seguridad pública, la defensa nacional o la salud pública».

De ello surge que es una de las fuentes de protección, aunque no con un nivel inferior al secreto de las fuentes de información periodísticas, ya que la ley es, acorde con la constitución de una claridad meridiana, al establecer que "en ningún caso" podrá afectarse el secreto de las fuentes de información periodística.

VII. LEY 25.326 DE PROTECCIÓN DE DATOS PERSONALES Y HÁBEAS DATA⁵⁶.

1. Antecedentes

Nuestro antecedente más concreto está en la Ley Española (LORTAD) "Ley Orgánica de Regulación del Tratamiento Automatizado de Datos" de 1992 –reemplazada en 1999 por la "Ley Orgánica de Protección de Datos de Carácter Personal"–. Sin embargo, en España son varias las normas que forman el sistema de protección de datos⁵⁷:

- a. La Ley 30/1992 (que dispone en su artículo 37.2 que «el acceso a los documentos que contengan datos referentes a la intimidad de las personas, estará reservado a éstas»; en su artículo 37.3 que «el acceso a los documentos de carácter nominativos que sin incluir otros datos pertenecientes a la intimidad de las personas figuren en los procedimientos de aplicación del derecho, salvo los de carácter sancionador o disciplinario, y que, en consideración a su contenido, puedan hacerse valer para el ejercicio de los derechos de los ciudadanos, podrá ser ejercido, además de por sus titulares, por terceros que acrediten un interés legítimo y directo», y en su artículo 37.6, que remite a otras disposiciones que establecen el secreto sobre determinadas categorías de documentos, como los que contengan

56. Todo este título ampliar de PUCCINELLI, Óscar Raúl, "Ley 25.326" –comentada–. Textos Legales Astrea Editorial, Astrea, marzo 2001.

57. FERNÁNDEZ RAMOS, *El derecho de acceso a los documentos administrativos*, Marcial Pons, Ediciones Jurídicas y Sociales S.A., Madrid, 1997, p. 491. Citado por PUCCINELLI, Óscar Raúl, *op. cit.* en nota al pie n. 57

datos sanitarios de los pacientes –Ley 14/1986, General de Sanidad y LORTAD, artículo 7.3–, los regulados por la legislación electoral –la LO-REG, artículo 41– y los que sirvan a fines estadísticos dentro del ámbito de la función pública estadística –la Ley 12/1989, de la Función Estadística Pública, artículos 13 y 19);

- b. La Ley Orgánica de Regulación del Tratamiento Automatizado de Datos (LORTAD), que reconoce, v. gr., un catálogo especial de datos de carácter personal en su artículo 7, en dos niveles de protección: los “hipersensibles”, constituidos por los datos que revelen ideología, religión o creencias, y los “sensibles”, que son los que denotan origen racial, salud y vida sexual. Ambos pueden ser tratados, pero en los primeros sólo con consentimiento expreso y por escrito, y en los segundos, sólo por disposición legal en atención a razones de interés general o por consentimiento expreso pero no necesariamente instrumentado por escrito (esta norma, valga recordarlo, fue sustituida por la Ley Orgánica de Protección de Datos de Carácter Personal de 1999);
- c. El Reglamento del Registro Civil, que tutela las informaciones relativas a la filiación personal;
- d. La Ley Básica de Régimen Local, tras la modificación introducida por Ley 4/1996, que en su artículo 16.3 protege los datos referidos al lugar y fecha de nacimiento o a la titulación académica que se posea, obrantes en el padrón municipal, y
- e). La Ley 2/1991, sobre derechos de información de los representantes de los trabajadores en materia de contratación, que cubre el estado civil, el DNI e incluso el domicilio.

Aunque hay otros antecedentes de menor importancia, a los efectos de nuestra ley, entre ellos: la Ley Francesa 78-17 del 6 de enero de 1978; en Estados Unidos la *Privacy Protection Act* de 1980; Brasil sancionó la Ley 9507 de reglamentación de acceso a la información y el procedimiento de *habeas data* el 12 de noviembre de 1997; y recientemente en Chile, en agosto de 1999, se sanciona la Ley 19.628 sobre protección de la vida privada, que reglamenta el tratamiento de los datos de carácter personal⁵⁸.

Si bien ha habido varios proyectos de *habeas data*, después de la reforma constitucional de 1994; y aún antes, consideramos que los más significativo fueron: a) el que llegó a ser Ley 24.745 sancionada por el Congreso de la Nación en 1996. Sin embargo, fue totalmente vetada por el Poder Ejecutivo

58. SLAJBE, María Eugenia; GABOT, Claudio, “*Habeas data*: su alcance en la legislación comparada y en nuestra jurisprudencia”. *La Ley* “Suplemento de Derecho Constitucional”, 17 de marzo de 2000.

Nacional a través del Decreto 1616/96, en relación con los artículos 5, 16, 35 y 36. Dicha ley también tomaba como fuente principal la LORTAD, o Ley Española de Protección de Datos, de 1992; puesto que la misma fue reformada en 1999; y, b) el que en noviembre de 1998 logra media sanción en el Senado; de autoría del senador Menem⁵⁹.

2. La Ley 25.326. Consideraciones generales

La ley fue sancionada el 4 de octubre de 2000; promulgada parcialmente el 30 de octubre de 2000; y publicada en el *Boletín Oficial* el 2 de noviembre de 2000.

La misma se divide en VII capítulos que describimos a continuación:

Capítulo I. Disposiciones Generales: Artículo 1° –(Objeto); **artículo 2°** –(Definiciones).

Capítulo II. Principios generales relativos a la protección de datos: Artículo 3° –(Archivos de datos – Licitud); **artículo 4°** –(Calidad de los datos); **artículo 5°** –(Consentimiento); **artículo 6°** –(Información); **artículo 7°** –(Categoría de datos); **artículo 8°** –(Datos relativos a la salud); **artículo 9°** –(Seguridad de los datos); **artículo 10.** –(Deber de confidencialidad); **artículo 11.** –(Cesión); **artículo 12.** –(Transferencia internacional).

Capítulo III. Derechos de los titulares de datos: Artículo 13. –(Derecho de Información); **artículo 14.** –(Derecho de acceso); **artículo 15.** –(Contenido de la información); **artículo 16.** –(Derecho de rectificación, actualización o supresión); **artículo 17.** –(Excepciones); **artículo 18.** –(Comisiones legislativas); **artículo 19.** –(Gratuidad); **artículo 20.** –(Impugnación de valoraciones personales).

Capítulo IV. Usuarios y responsables de archivos, registros y bancos de datos: Artículo 21. –(Registro de archivos de datos. Inscripción); **artículo 22.** –(Archivos, registros o bancos de datos públicos); **artículo 23.** –(Supuestos especiales); **artículo 24.** –(Archivos, registros o bancos de datos privados); **artículo 25.** –(Prestación de servicios informatizados de datos personales); **artículo 26.** –(Prestación de servicios de información crediticia); **artículo 27.** –(Archivos, registros o bancos de datos con fines de publicidad); **artículo 28.** –(Archivos, registros o bancos de datos relativos a encuestas).

Capítulo V. Control: Artículo 29. –(Órgano de Control); **artículo 30.** –(Códigos de conducta).

Capítulo VI. Sanciones: Artículo 31. –(Sanciones administrativas); **artículo 32.** –(Sanciones penales).

Capítulo VII. Acción de protección de los datos personales: Artículo 33. –(Procedencia); **artículo 34.** –(Legitimación activa); **artículo 35.** –(Legitimación pasiva);

artículo 36. –(Competencia); **artículo 37.** –(Procedimiento aplicable); **artículo 38.** –(Requisitos de la demanda); **artículo 39.** –(Trámite); **artículo 40.** –(Confidencialidad de la información); **artículo 41.** –(Contestación del informe); **artículo 42.** –(Ampliación de la demanda); **artículo 43.** –(Sentencia); **artículo 44 y 45** –(Ambito de aplicación); **artículo 46.** –(Disposiciones transitorias); **artículo 47; artículo 48.** –Comuníquese al Poder Ejecutivo.

Si bien excede los límites del presente trabajo se realiza un estudio pormenorizado de la norma, además de las disposiciones que en cada título hemos considerado necesario resaltar, debemos puntualizar algunas cuestiones.

La presente ley establece, en su **artículo 1°**, el **objeto** de la misma: fue sancionada con miras a la protección integral de los datos personales asentados en archivos, registros o bancos de datos públicos o privados destinados a dar informes, con el objeto de garantizar el derecho al honor y la intimidad de las personas. Por lo tanto, no resulta aplicable a otros registros de información que tienen distintas finalidades; por ejemplo, los periodísticos, culturales o científicos, que se mantienen dentro de un ámbito de absoluta intimidad. Ello no es perfectamente coherente con el bien jurídico que se pretende tutelar; sino con el fin de proteger el derecho a la intimidad. Estaríamos también vulnerando el mismo derecho; tal el caso si se permitiera el acceso a registros privados “no destinados a proveer informes”. La norma aquí pretende enunciar el objeto de la ley, pero en realidad parece caer en el error común de confundir “objeto” con lo que en realidad constituye el “objetivo” de la ley –los propósitos que animan al legislador. Además, este artículo sigue en esencia el diseño del artículo 1° de la ya derogada LORTAD española de 1992 –con adaptaciones propias al artículo 43 de la Constitución Nacional– y por ello incurre en el error de limitar la garantía a la protección del derecho al “honor” y a la “intimidad” de las personas. Que, además de ser incorrecta la referencia a un “derecho al honor y a la intimidad”, pues se trata de dos derechos que, aunque puedan estar íntimamente vinculados, son diferentes, ya hemos sentado nuestra postura en el sentido de considerar que se protege una amplia gama de derechos y no se “acota” a lo establecido en la norma.

El **artículo 1°** dispone en su segundo párrafo que

«Las disposiciones de la presente ley también serán aplicables, en cuanto resulte pertinente, a os datos relativos a personas de existencia ideal».

Compartimos las opiniones vertidas por Puccinelli; por un lado, si bien se hubiera preferido el rótulo “personas jurídicas” por considerarlo un sinónimo más apropiado de “persona de existencia ideal”, el legislador –*no sabemos si conscientemente o no, pues ello no sale de los debates*– adoptó correctamente la segunda denominación mencionada. Y ello es así, ya que sin duda es la única que puede ser considerada abarcativa de todos los supuestos que pretende incluir (género) y no llevaría a equívocos interpretativos (recordemos

que para alguna doctrina, v. gr., Llambías, las personas de existencia ideal pueden dividirse entre "personas de existencia ideal propiamente dichas" -v. gr.: un consorcio, una simple asociación- y "personas jurídicas" -v. gr., una sociedad anónima; y que ello no ocurre con las personas de existencia visible, cuyo único supuesto lo constituyen las personas físicas).

El autor expresa que

«lo que puede llevar a amputaciones innecesarias de las facultades reconocidas por la ley es la frase "en cuanto resulte pertinente" cuando intenta definir los supuestos en que se tutelan los derechos de las personas de existencia ideal.

¿Quiere decir que sólo cubriría los derechos que pueden ostentar las personas de existencia ideal? Consecuentemente, ¿tienen honor o intimidad estas personas que puedan ser protegidas por la ley? ¿Sólo se cubriría el derecho de "acceso a la información que sobre las mismas se registre"»?

La cuestión fue objeto de debate y, en este sentido, el senador Menem explicó:

«El régimen se hace extensivo a la protección de los datos de las personas de existencia ideal, inclusión que se efectúa no sólo porque existen antecedentes en ese sentido en el derecho comparado, sino porque además el artículo 43 se refiere a toda persona, sin distinguir entre personas de existencia física e ideal. Y recordemos, además, que hay un precepto jurídico según el cual donde la ley no distingue no debemos distinguir. Es cierto que alguien podría preguntar, válidamente, cómo se puede proteger el derecho a la intimidad de una persona ideal. Sin embargo, no es que se trate de proteger la intimidad de este tipo de personas sino de su derecho a que se tenga de ellas un conocimiento adecuado y real; que no sean objeto de discriminación ni de información que las pueda colocar en una situación difícil. Además, no cabe duda de que las personas de existencia ideal están integradas por personas de existencia física. Y muchas veces, la información que afecta a una persona de existencia ideal puede afectar, indirectamente, a las personas de existencia física que la integran. Sería el caso de una sociedad de la cual se diga que ejerce actividades ilícitas o de contrabando. Indudablemente, quienes integren dicha sociedad se verán afectadas por el se dato falso. Por eso, también hemos incluido la protección de las personas de existencia ideal»⁶⁰.

De apoyarnos en esta explicación, obviamente la aparente obturación que podría surgir de una perspectiva literal se diluye, y podemos afirmar sin dudas que respecto de las personas jurídicas, la ley cubre con la misma extensión que lo hace acerca de las personas físicas, y no sólo porque pueden estar integrados por personas físicas, sino porque algunos derechos de aquella son similares (bien puede decirse que si bien las personas jurídicas no tienen estrictamente "honor", sí tienen, v. gr., determinada reputación en el medio, y si tal vez tampoco tienen estrictamente "intimidad", sí tienen un derecho de reserva acerca determinados aspectos, como la índole y contenido de sus operaciones»⁶¹.

60. Antecedentes Parlamentarios, La Ley, año 7, n. 11, Buenos Aires, 2000, pp. 361-362. Citado por PUCCINELLI, Óscar Raúl, *op. cit.* en nota al pie n. 57.

61. PUCCINELLI, Óscar Raúl, *op. cit.* en nota al pie n. 57.

Resulta de gran importancia el 2º artículo; puesto que en el mismo están contenidas las definiciones y el significado de los conceptos que se manejarán en toda la norma; el mismo establece:

A los fines de la presente ley se entiende por: **-Datos personales:** Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables. **-Datos sensibles:** Datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual. **-Archivo, registro, base o banco de datos:** Indistintamente, designan al conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso. **-Tratamiento de datos:** Operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, y en general el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias. **-Responsable de archivo, registro, base o banco de datos:** Persona física o de existencia ideal pública o privada, que es titular de un archivo, registro, base o banco de datos. **-Datos informatizados:** Los datos personales sometidos al tratamiento o procesamiento electrónico o automatizado. **-Titular de los datos:** Toda persona física o persona de existencia ideal con domicilio legal o delegaciones o sucursales en el país, cuyos datos sean objeto del tratamiento al que se refiere la presente ley. **-Usuario de datos:** Toda persona, pública o privada que realice a su arbitrio el tratamiento de datos, ya sea en archivos, registros o bancos de datos propios o a través de conexión con los mismos. **-Disociación de datos:** Todo tratamiento de datos personales de manera que la información obtenida no pueda asociarse a persona determinada o determinable.

Es importante destacar que la norma exige que el titular de los datos preste su consentimiento.

«**Artículo 5º** (Consentimiento). 1. El tratamiento de datos personales es ilícito cuando el titular no hubiere prestado su consentimiento libre, expreso e informado, el que deberá constar por escrito, o por otro medio que permita se le equipare, de acuerdo a las circunstancias. El referido consentimiento prestado con otras declaraciones, deberá figurar en forma expresa y destacada, previa notificación al requerido de datos, de la información descrita en el artículo 6º de la presente ley. 2. No será necesario el consentimiento cuando: a) Los datos se obtengan de fuentes de acceso público irrestricto; b) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal; c) Se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio; d) Deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento; e) Se trate de las operaciones que realicen las entidades financieras y de las informaciones que reciban de sus clientes conforme las disposiciones del artículo 39 de la Ley 21.526».

Se crea un organismo de control (**artículo 29**) al que pueden recurrir para recibir asesoramiento todas aquellas personas que se sientan afectadas y

requieran la defensa de los derechos que esta ley garantiza. Este mismo organismo está facultado para imponer severas sanciones a las empresas que violen sus disposiciones haciendo abuso de los datos.

«**Órgano de Control**). "1. El órgano de control deberá realizar todas las acciones necesarias para el cumplimiento de los objetivos y demás disposiciones de la presente ley. A tales efectos tendrá las siguientes funciones y atribuciones: a) Asistir y asesorar a las personas que lo requieran acerca de los alcances de la presente y de los medios legales de que disponen para la defensa de los derechos que ésta garantiza; b) Dictar las normas y reglamentaciones que se deben observar en el desarrollo de las actividades comprendidas por esta ley; c) Realizar un censo de archivos, registros o bancos de datos alcanzados por la ley y mantener el registro permanente de los mismos; d) Controlar la observancia de las normas sobre integridad y seguridad de datos por parte de los archivos, registros o bancos de datos. A tal efecto podrá solicitar autorización judicial para acceder a locales, equipos, o programas de tratamiento de datos a fin de verificar infracciones al cumplimiento de la presente ley; e) Solicitar información a las entidades públicas y privadas, las que deberán proporcionar los antecedentes, documentos, programas u otros elementos relativos al tratamiento de los datos personales que se le requieran. En estos casos, la autoridad deberá garantizar la seguridad y confidencialidad de la información y elementos suministrados; f) Imponer las sanciones administrativas que en su caso correspondan por violación a las normas de la presente ley y de las reglamentaciones que se dicten en su consecuencia; g) Constituirse en querrelante en las acciones penales que se promovieran por violaciones a la presente ley; h) Controlar el cumplimiento de los requisitos y garantías que deben reunir los archivos o bancos de datos privados destinados a suministrar informes, para obtener la correspondiente inscripción en el Registro creado por esta ley. 2. El órgano de control gozará de autonomía funcional y actuará como órgano descentralizado en el ámbito del Ministerio de Justicia y Derechos Humanos de la Nación. 3. El órgano de control será dirigido y administrado por un Director designado por el término de cuatro (4) años, por el Poder Ejecutivo con acuerdo del Senado de la Nación, debiendo ser seleccionado entre personas con antecedentes en la materia. El Director tendrá dedicación exclusiva en su función, encontrándose alcanzado por las incompatibilidades fijadas por ley para los funcionarios públicos y podrá ser removido por el Poder Ejecutivo por mal desempeño de sus funciones».

En relación con Registros de antecedentes, el senador Menem expresó:

«El nuevo texto legal se aplica también a los registros públicos, por lo que el registro permanente y el tratamiento de datos personales con fines de defensa nacional o seguridad pública por parte de las Fuerzas Armadas, fuerzas de seguridad, organismos policiales o inteligencia están sometidos al nuevo régimen legal que obliga a respetar la confidencialidad, limita la cesión de los datos y permite el acceso a ellos del interesado para verificar su exactitud. La incorporación de estos registros tiene por objeto evitar el mantenimiento por parte de esas fuerzas de datos que no resulten imprescindibles para su función, por ejemplo aquellos datos que la ley denomina sensibles, que son los que revelan el origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.

Por otra parte, la ley expresamente establece que no se altera de ningún modo el registro de antecedentes penales o contravencionales, que se registrarán por la legislación específica que los regula, cuyo pleno funcionamiento queda así garantizado de modo que la Justicia pueda disponer de amplia información para evaluar la eventual reincidencia del imputado.

Es decir, la ley de *hábeas data* no flexibiliza ni permite de ninguna manera la alteración de aquellos datos que hacen a la seguridad pública, los que se mantendrán registrados por los plazos y en las condiciones que prevén las leyes especiales que los rigen, sin que nadie que tenga antecedentes penales pueda beneficiarse de algún modo por esta nueva ley.

Un caso especial está constituido por las empresas dedicadas a brindar información crediticia, las que sólo podrán mantener en sus registros datos de carácter patrimonial relativos a la solvencia económica. En cuanto a la información de deudores que hayan cumplido sus obligaciones, se prevé que los datos se mantendrán por el plazo de dos años. Así, alguien que tuvo un atraso en un pago hace tres años, que luego regularizó, deberá ser eliminado del registro, con lo que se evita la injusta situación actual, que al mantenerlo por largo tiempo le impide acceder al crédito.

Por única vez, la ley establece una especie de blanqueo, ya que las empresas deberán suprimir de sus registros todo dato referido a incumplimientos de obligaciones ya extinguidas en el momento de la sanción de esta ley⁶².

Siguiendo a Puccinelli⁶³, consideramos que

«A tenor de lo dispuesto por el artículo 44 de la ley, ésta resulta de aplicación en toda la República, salvo en lo que respecta al órgano de control; la inscripción de los códigos de conducta; las sanciones administrativas; la obligación de inscripción en los registros de los archivos existentes al momento de la sanción de la ley, y la acción de protección de datos personales –excepto cuando para tramitarla corresponda la competencia federal, a tenor del artículo 36 de la ley–. Quedan así para los estados federados la regulación de los aspectos no abarcados por la norma federal. Acerca de la conveniencia de la fórmula escogida por el legislador, indica Gozaini que es correcto que una norma de este tipo adopte regulaciones generales para toda la República, aunque debe respetar el criterio establecido por el artículo 5 de la Constitución Nacional, que reconoce la autonomía provincial, y Montoto Guerreiro observa que: a) no es delegable, a nivel nacional, la protección de la autodeterminación informativa, razón por la cual los estados locales deben implementar las medidas no jurisdiccionales (administrativas) tendientes a asegurar su efectivo respeto, y b) debería estar regulado por una ley federal el tráfico interprovincial de datos (ya que corresponde al Congreso, por el artículo 75 inciso 13 constitucional “reglar el comercio de las provincias entre si...”), como así también regular el funcionamiento y acceso a las bases nacionales e internacionales que posean datos de ciudadanos argentinos».

62. MENEM, Eduardo, “Una ley que garantiza el derecho al honor y a la intimidad”. *La Nación*; 30 octubre de 2000.

63. PUCCINELLI, Óscar Raúl, *op. cit.*, en nota al pie n. 57.

Es a nuestro criterio de destacar que la ley tipifica nuevos delitos; así el artículo 32 establece:

«**(Sanciones penales)** 1. Incorporase como artículo 117 bis del Código Penal, el siguiente: 1°. Será reprimido con la pena de prisión de un mes a dos años el que insertara o hiciera insertar a sabiendas datos falsos en un archivo de datos personales. 2°. La pena será de seis meses a tres años, al que proporcionara a un tercero a sabiendas información falsa contenida en un archivo de datos personales. 3°. La escala penal se aumentará en la mitad del mínimo y del máximo, cuando del hecho se derive perjuicio a alguna persona. 4°. Cuando el autor o responsable del ilícito sea funcionario público en ejercicio de sus funciones, se le aplicará la accesoria de inhabilitación para el desempeño de cargos públicos por el doble del tiempo que el de la condena. 2. Incorporase como artículo 157 bis del Código Penal el siguiente: Será reprimido con la pena de prisión de un mes a dos años el que: 1°. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales; 2°. Revelare a otro información registrada en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de una ley. Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de uno a cuatro años».

VIII. CONCLUSIONES

A nuestro criterio, es bien cierto que la ley adolece de varios errores; ellos fueron exhaustivamente detallados por Puccinelli y Sukerman⁶⁴; entre ellos: En el Capítulo IV, se observan incongruencias; como por ejemplo se invierten términos (v. gr., "usuarios y responsables" por "responsables o usuario" en los artículos 26, 30, 31), y falta de precisión, toda vez que en el caso del artículo 22.1 no queda muy claro si lo que se quiere es prohibir las leyes secretas para estos casos.

En el capítulo V, la ausencia de definición de estructura y financiamiento de la actividad del órgano de control –lo que implica una omisión del debido estudio de costos de toda tarea legislativa responsable– podría haber permitido superar el veto de los puntos 2 y 3 del artículo 29.

En el capítulo VII, se incluyen artículos que no condicen con la denominación del capítulo y que la técnica legislativa indica como habitual que se trate en capítulos distintos del que fueron incorporados; tal el caso del artículo 44 que se refiere al "ámbito de aplicación de la ley", que lo lógico sería que figure al comienzo del dispositivo legal, en las disposiciones preliminares no al final, pues el destinatario de la ley debe saber desde el principio –en el encabezado de la ley– el ámbito en que van a ser obligatorias dichas normas. También se

64. SUKERMAN, Roberto, «Técnica legislativa de la Ley 25.326», disertación pronunciada en el marco del Seminario "Introducción a la Técnica Legislativa", Facultad de Derecho, U.N.R., 2000.

podría haber creado otro capítulo bajo el nombre de "Disposiciones Transitorias" a partir del artículo 45.

«Finalmente, cabe remarcar que, resulta insólita e inexplicable la decisión de nombrar a la garantía como "acción de protección de los datos personales o de *hábeas data*". Los institutos jurídicos no pueden tener dos nombres ¿o *hábeas data* será un apodo?, y que, también sorprendentemente, los artículos 45 y 47 son los únicos que están sin epigrafiar⁶⁵.

Sin embargo, en líneas generales, consideramos que la ley cubre el requerimiento social estableciendo una solución, por un lado, a los aspectos relacionados con la regulación de los archivos de datos de personas físicas y de existencia ideal; y, por el otro, de la regulación de bancos o registros de datos, privados, destinados a proveer informes, o públicos, en las condiciones establecidas por la presente ley.

Creemos, como ya lo resaltáramos en otra parte del presente trabajo, que se ha logrado un equilibrio entre el derecho a la información y el derecho a la intimidad; que son, en definitiva, los bienes en pugna, que, esta garantía debe "equilibrar".

La ley tiene aspectos que resultan a nuestro entender plenamente satisfactorios.

Queda plenamente justificada la necesidad de pormenorizar definiciones en el artículo 2º; puesto que se trata de un tema con bastantes aspectos técnicos y relativamente novedosos. Además, guarda coherencia con las técnicas utilizadas en el caso en el derecho comparado.

La ley no se aparta de la norma constitucional cuando se refiere a las posibilidades que, a partir de ellas, tendrán los dueños de los datos; se permitirá: 1) que una persona pueda acceder a la información que sobre ella conste en un registro o banco de datos, como también la finalidad de su registro; 2) que se actualicen datos atrasados; 3) que se rectifiquen los datos inexactos; 4) que se asegure la confidencialidad, impidiendo que ciertos datos se transfieran ilegítimamente a terceros, y 5) se prohíbe el registro de información sensible, que es fundamentalmente la relativa a ideas políticas, religión, raza y hábitos sexuales, en la medida en que importe discriminación de las personas

La protección a la intimidad de los datos personales se completa con la tipificación de nuevas figuras delictivas en el ámbito de la informática; tal el caso de: 1) el que insertara o hiciere insertar a sabiendas datos falsos en archivos de datos personales; 2) el que proporcione, a sabiendas información falsa de

65. SUKERMAN, Roberto, cit. n. 65.

un tercero; 3) se aumenta la pena, cuando el hecho culmine con un daño efectivo a un tercero; 4) asimismo se agravará la pena si quien comete el delito es un funcionario en ejercicio de sus funciones; 5) también quien violare sistemas de seguridad o confidencialidad para acceder a datos de otras personas, cuyo secreto debiera preservar.

El proceso judicial es una "acción de amparo especial"; con esto no se aparta la ley de la Constitución; el trámite es rápido (los bancos de datos, salvo prórroga del juez, deberán contestar dentro de los 5 días hábiles –artículo 39–), pero salvaguarda la esencia de la garantía, puesto que a diferencia de la acción de amparo del 1º párrafo del **artículo 43**, no se requiere "arbitrariedad o ilegalidad manifiesta"; condiciones *sine qua non* para la procedencia de la acción "común" de amparo.

Por último, es necesario reflexionar que en la mayoría de las leyes de derecho comparado en relación con este tema, y aún la LORTAD, fuente de inspiración de nuestra norma, la acción de *hábeas data* es "personalísima"; esto es, sólo puedo conocer mis datos personales y los de ninguna otra persona; con la muerte del titular del dato, muere la posibilidad de conocer el mismo.

Nuestra ley siguiendo el mencionado fallo *Urteaga*; teniendo especialmente en cuenta la historia de nuestro país en las últimas décadas, decide incorporar en el **artículo 34** la legitimación activa, extendiéndola al «afectado, sus tutores o curadores y sucesores de las personas físicas, sea en línea recta o colateral hasta el segundo grado, por sí o por apoderado». Con lo cual los legisladores han demostrado continuar el criterio "aperturista" de nuestros tribunales, y en definitiva lo que es más importante aún, cumplir con los requerimientos de la sociedad.

