

EL SISTEMA DE PROTECCIÓN DE DATOS PERSONALES EN LA CIUDAD AUTÓNOMA DE BUENOS AIRES

Marcela I. BASTERRA ¹

I. Introducción

El avance de las nuevas tecnologías implica una constante inquietud para el análisis de la inserción de la informática en el ámbito jurídico. La discusión se ha instalado en la agenda de los sistemas normativos, y mantendrá vigencia mientras continúe desarrollándose este proceso global. Constituye, sin duda, uno de los temas fundamentales a considerar dentro de esta temática, la protección jurídica de los derechos individuales a la luz de los avances tecnológicos ².

Las personas que viven en una sociedad tecnológicamente desarrollada, a diario proporcionan determinada información acerca de sí mismas, como el domicilio, número de documento, profesión, miembros que integran su familia, si poseen tarjetas de créditos o cuenta bancaria, si tienen automóvil, estudios cursados, informes relacionados con su patrimonio, etc. ³.

Lo que caracteriza al dato personal es precisamente la posibilidad de identificar con alguna precisión a la persona -física o jurídica- a la que esa información pertenece. Esta posibilidad es lo que origina la protección, ya que a través del dato se puede llegar no sólo

1 Marcela I. BASTERRA. Doctora en Derecho (UBA). Magíster en Derecho Constitucional y Derechos Humanos. Profesora de grado, posgrado y doctorado de Derecho Constitucional en UBA, UCA y UCES, entre otras varias universidades. Presidenta del Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires.

2 BASTERRA, Marcela I., “Datos personales para fines publicitarios. A propósito de la Disposición 4/2009 de la Dirección Nacional de Protección de Datos Personales”, La Ley, 2009-B, p. 1037. Cita Online: AR/DOC/1357/2009.

3 BASTERRA, Marcela I., “Obligaciones de los responsables de los bancos de datos. El estándar de calidad de la información”, La Ley 2014-F, p. 91, Cita Online: AR/DOC/3448/2014.

a la persona, sino incluso a establecer conductas y prácticas que únicamente mediando la expresa voluntad del titular del dato, pueden trascender la esfera de su intimidad ⁴.

Los continuos desafíos informáticos obligan a abandonar el concepto de intimidad como libertad negativa, exigiendo avanzar hacia una fase activa del proceso de circulación de la información personal al brindar protagonismo al interesado, posibilitándole el ejercicio de un adecuado control para la preservación de su libertad informática, espectro en cuyo interior subyace la nota de exigencia de veracidad y precisión de la información que le concierne ⁵.

Estos nuevos fenómenos sociales dieron lugar a un nuevo derecho fundamental derivado de la intimidad; la autodeterminación informativa ⁶. Siguiendo esa línea argumental, podemos considerar al derecho a la autodeterminación informativa como el fundamento de la protección de los datos personales.

Este derecho consiste en la posibilidad que tiene el titular de un dato a controlar quiénes serán destinatarios de su información personal y qué uso se dará a la misma. Se ejerce genéricamente a través de los derechos de acceso, rectificación, supresión, confidencialidad y cancelación ⁷.

Según BIDART CAMPOS ⁸, la doctrina y el Derecho comparado en materia de habeas data tienen su punto de partida en el derecho personal a conocer los propios datos, que existan en registros o ban-

4 BASTERRA, Marcela I., “Aspectos constitucionales de la protección de datos personales”, en TRAVIESO, Juan Antonio (director), *Régimen jurídico de los datos personales*, Abeledo-Perrot, Ciudad Autónoma de Buenos Aires, 2014, t. I, p. 82.

5 BASTERRA, Marcela I., “La responsabilidad de los motores de búsqueda de Internet en el centro del debate jurídico”, *La Ley* 2014-F, p. 145. Cita Online: AR/DOC/4087/2014.

6 SANTOS, Estefanía, “Las redes sociales: Desafíos para la protección de datos personales”, en TRAVIESO, Juan Antonio (director), *Régimen jurídico de los datos personales*, p. 569.

7 BASTERRA, Marcela I., *Protección de Datos Personales. Ley 25.326 y Dto. 1558/01 Comentados. Derecho Constitucional Provincial, Iberoamérica y México*, Ediar, Buenos Aires y Editorial UNAM, México, 2008, p. 11.

8 BIDART CAMPOS, Germán, “¿Habeas data, o qué? ¿Derecho a la verdad, o qué?”, *La Ley* 1999-A, p. 212. Cita Online: AR/DOC/14974/2001.

cos de datos. De ahí en más, una vez conocidos éstos se podrá proceder a modificarlos, rectificarlos, ampliarlos, proteger los datos sensibles, suprimirlos, actualizarlos, impedir su divulgación, etc.

Las facultades de disposición y control son el fundamento que sostiene la estructura legal de la protección de los datos personales. En estas facultades se arraigan los requisitos y principios de licitud de tratamiento de datos, como lo son el consentimiento previo y los derechos de oposición, acceso, rectificación y supresión de la información personal, entre otros. La protección de la información personal es la respuesta del derecho a la nuevas tecnologías, permitiendo transpolar la garantía del habeas corpus al habeas data: del tengo mi cuerpo al tengo mis datos, para controlarlos y determinarlos ⁹.

Sin duda, esta garantía y a través de la misma el derecho a la protección de los datos personales -entendida como la rama del Derecho que protege la autodeterminación informativa-, aparecen como un punto de partida que marcará para siempre un hito en la regulación de la informática y las comunicaciones ¹⁰.

En este trabajo analizaremos la regulación del habeas data en la Ciudad de Buenos Aires, y haremos una breve mención a distintos supuestos que implican un desafío para esta garantía.

II. El habeas data en la Ciudad Autónoma de Buenos Aires. Protección constitucional

La Constitución porteña regula el habeas data en el Título primero “Derechos y Garantías”, del Libro primero “Derechos, garantías y políticas especiales”. Esta fue sancionada en el año 1996, lo que explica que se tomara como fuente la fórmula federal, establecida en el artículo 43 a través de la reforma de 1994.

Así, el artículo 16 señala: *“Toda persona tiene, mediante una acción de amparo, libre acceso a todo registro, archivo o banco de datos que conste en organismos públicos o en los privados destinados a*

9 GONZÁLEZ ALLONCA, Juan Cruz, “Los buscadores de internet y la ley de protección de datos personales”, La Ley 2014-D, p. 715, Cita Online: AR/DOC/2108/2014.

10 BASTERRA, Marcela I., *Protección de Datos Personales. Ley 25.326 y Dto. 1558/01 Comentados. Derecho Constitucional Provincial, Iberoamérica y México*. p. 11.

proveer informes, a fin de conocer cualquier asiento sobre su persona, su fuente, origen, finalidad o uso que del mismo se haga.

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

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

En forma expresa la norma establece al de habeas data como una acción de amparo y no como una figura autónoma. Si examinamos el 2° párrafo del artículo 16, prevé en forma explícita que la actualización, rectificación, confidencialidad o supresión esté supeditada a que esa información lesione o restrinja algún derecho. En este punto, consideramos que la fórmula local tiene inferiores estándares de protección tuitiva que la norma federal, dado que de la interpretación de esta última surge que no es necesario que el individuo que exige la supresión de información personal demuestre lesión a derecho alguno, ni tampoco que el mismo va a ser utilizado con fines discriminatorios, basta únicamente que sea un dato sensible o falso para que se solicite la supresión ¹¹.

Tampoco debe probarse restricción o cercenamiento de derechos en relación a los datos “obsoletos”, pudiendo igualmente solicitar la actualización de los mismos. De cualquier forma, la Constitución Nacional tiene jerarquía superior a las normas provinciales y en este caso a las de la Ciudad. En ese sentido, la ley reglamentaria del artículo 43, 3° párrafo N° 25.326 ¹², en el artículo 16. 1 establece “*Toda persona tiene derecho a que sean rectificadas, actualizados y, cuando corresponda, suprimidos o sometidos a confidencialidad los datos personales de los que sea titular, que estén incluidos en un banco de datos*”. Como se advierte no exige que exista lesión o restricción a derecho alguno ¹³.

11 BASTERRA, Marcela I., “Derecho a la Intimidad y Habeas Data en la Ciudad Autónoma de Buenos Aires” en BIDART CAMPOS, Germán y GIL DOMÍNGUEZ, Andrés (directores), *Instituciones de la Ciudad Autónoma de Buenos Aires*, La Ley, Buenos Aires, 2001, p. 76.

12 Ley N° 25.326, publicada en el B.O. del 02/11/2000.

13 Puede verse de BASTERRA, Marcela I., “Derecho a la Intimidad y Habeas Data en la Ciudad...”, cit., pp. 69-95.

Asimismo, se ha señalado que la garantía que reconoce la Constitución local es diferente a la que establece la nacional en el artículo 43, ya que mientras “(...) la ciudad se ocupa de otorgar un derecho autónomo destinado a controlar el tratamiento de datos personales referidos a personas físicas o de existencia ideal, asentados o destinados a ser asentados en archivos, registros, bases o bancos de datos, el sistema nacional reduce el alcance de los archivos fiscalizados ya que solamente asigna la garantía contra las bases de datos destinadas a proporcionar información a terceros”¹⁴.

En otras jurisdicciones, por ejemplo en la Provincia de Buenos Aires, se consagra esta garantía en forma expresa en el inciso 3° del artículo 20 constitucional. La fórmula específica que se trata de una *acción de habeas data* y determina que tramitará según el procedimiento que establezca la ley reglamentaria; es decir, que no se confunde o se crea como una acción de amparo, error en el que incurrieron tanto la Constitución Nacional como la de la Ciudad¹⁵.

En relación a los tipos de habeas data enmarcándolos en la clasificación de SAGÜÉS¹⁶, se establece en la Ciudad un *habeas data informativo*, con sus sub-tipos; *habeas data exhibitorio* “Toda persona -física o jurídica- podrá conocer lo que conste de la misma...”; *habeas data finalista* “...así como la finalidad a que se destine la información...”. Aquí además, se amplía al conocimiento de la fuente y el origen del dato.

En cuanto a la posibilidad de revertir la situación a través de este instituto, se prevé -igual que en la normativa nacional- *el habeas data rectificador, habeas data aditivo y habeas data cancelatorio o exclutorio*, según corresponda.

14 GOZAÍNI, Osvaldo Alfredo, “El habeas data en la Constitución de la Ciudad Autónoma de Buenos Aires”, en BASTERRA, M. (editora) *Constitución de la Ciudad Autónoma de Buenos Aires, Edición Comentada*, Jusbaire, Ciudad Autónoma de Buenos Aires, 2016, p. 239.

15 BASTERRA, Marcela I., *Protección de Datos Personales. Ley 25.326 y Dto. 1558/01 Comentados. Derecho Constitucional Provincial, Iberoamérica y México*, pp. 125 y 126.

16 SAGÜÉS, Néstor Pedro, “Subtipos de Habeas Data en el Derecho Argentino” en *Leyes Reglamentarias de la Reforma Constitucional*, Asociación Argentina de Derecho Constitucional, Buenos Aires, 1996, pp. 206-208.

El constituyente porteño ha querido también salvaguardar el secreto de la fuente de información periodística como en la normativa nacional, buscando un equilibrio razonable que no vulnere la libertad de expresión ¹⁷.

En “Bahhourí c/Gobierno de la Ciudad Autónoma de Buenos Aires” ¹⁸ la Cámara de Apelaciones en lo Contencioso administrativo y Tributario de la Ciudad, decidió que “es procedente la acción de habeas data tendiente a obtener la rectificación de la información que contiene la Dirección General de Rentas de la Ciudad Autónoma de Buenos Aires respecto de una deuda que se encuentra prescripta -en el caso, por patentes-, toda vez que le asiste al actor el derecho a que se haga constar en la base de datos de la demandada que la deuda ya no es exigible por tratarse de una obligación natural”.

En el caso, un contribuyente promovió acción de habeas data contra el Gobierno de la Ciudad -D.G.R.- con la finalidad de obtener la rectificación del registro referido a un automóvil de su propiedad, basando su petición en el hecho de que la deuda de patentes se hallaba prescripta. En primera instancia se hizo lugar a lo solicitado, ordenando a la demandada rectificar los datos y expedir constancia de libre deuda. La Cámara confirma la sentencia apelada, aunque con la aclaración de que no habrá de expedirse una constancia de libre deuda, sino una de deuda no exigible por tratarse de una obligación natural.

Con posterioridad, en el año 2014, la Sala III de la misma Cámara ratificó este criterio, es decir, que procede la acción de habeas data para solicitar la prescripción de deudas cuando de la prueba surgiera en forma manifiesta su procedencia y se hubiera garantizado a la demanda la posibilidad de debate y prueba ¹⁹.

17 LÓPEZ ALFONSÍN, Marcelo A., *Constitución de la Ciudad Autónoma de Buenos Aires Comentada*, Editorial Estudio, Buenos Aires, 1997, p. 66.

18 Cámara Contencioso administrativo y Tributario de la Ciudad Autónoma de Buenos Aires, Sala I: “Bahhourí, Graciela c. Gobierno de la Ciudad Autónoma de Buenos Aires”, 08/11/2002. La Ley 2003-B, p. 744.

19 Cámara Contencioso administrativo y Tributario de la Ciudad Autónoma de Buenos Aires, Sala III: “Guzmán, Héctor Alejandro c. GC BA”, 26/05/2014. La Ley Online, Cita Online: AR/JUR/30617/2014.

III. Ley A - N° 1.845 de Protección de Datos Personales ²⁰. Jurisprudencia

a. *Legitimación activa*

La normativa otorga legitimación activa, tanto a personas físicas como a personas de existencia ideal; en el último caso la acción deberá ser interpuesta por sus representantes legales o sus apoderados.

Establece una legitimación amplia en cuanto faculta a interponer la acción de protección de datos personales; al afectado, sus tutores o curadores como también a los sucesores en línea directa o colateral hasta el segundo grado.

En cuanto a la legitimación pasiva, dispone que la acción de habeas data procederá respecto de los responsables y/o encargados de tratamiento de archivos, registros o bancos de datos del sector público de la Ciudad Autónoma de Buenos Aires.

b. *Bancos o bases de datos comprendidos*

La ley tiene por objeto regular dentro del ámbito de la Ciudad, el tratamiento de datos personales referidos a personas físicas o de existencia ideal, asentados o destinados a ser asentados en archivos, registros, bases o banco de datos del sector público de la CABA.

En tal sentido, establece que se consideran incluidos dentro del sector público de la Ciudad a todos los archivos, registros, bases o bancos de datos de titularidad de los órganos pertenecientes a la Administración central, descentralizada, de entes autárquicos, empresas y sociedades del Estado, sociedades anónimas con participación estatal mayoritaria, sociedades de economía mixta y todas aquellas otras organizaciones empresariales en las que el Estado de la Ciudad de Buenos Aires tenga participación en el capital o en la formación de las decisiones societarias. También las existentes en el ámbito de los poderes Legislativo y Judicial en cuanto a su actividad administrativa, y de los demás órganos establecidos en el Libro II de la Constitución de la CABA.

²⁰ Ley A - N° 1.845 de la Ciudad Autónoma de Buenos Aires, publicada en el B.O.C.B.A del 03/08/2006.

c. Tipos de datos

En cuanto a la calidad de la información, la ley establece los siguientes lineamientos:

a) Los datos personales que se recojan a los efectos de su tratamiento deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido.

b) La recolección de información no puede hacerse por medios desleales, fraudulentos o en forma contraria a las disposiciones de la ley en estudio, como tampoco podrán ser utilizados para finalidades distintas de aquellas que motivaron su obtención.

c) Los datos deben ser exactos y actualizados, para que en caso que sea necesario poder responder con veracidad a la situación reclamada por su titular.

d) Los datos total o parcialmente inexactos o que sean incompletos, deben ser suprimidos y sustituidos, o en su caso completados por el responsable o usuario del archivo, registro, o banco de datos cuando se tenga conocimiento de la inexactitud o carácter incompleto de la información de que se trate, sin perjuicio de los derechos que la ley le otorga al titular.

e) Toda información personal deben ser destruida cuando haya dejado de ser necesaria o pertinente a los fines para los cuales hubiese sido recolectada, sin necesidad del requerimiento del titular de la misma ²¹.

La ley establece un principio general -en consonancia con la normativa nacional (art. 5)-, en virtud del cual se considera ilícito el tratamiento de datos personales cuando el titular no hubiere prestado su consentimiento libre, expreso e informado, el que deberá constar por escrito o por otro medio que se le equipare de acuerdo a las circunstancias.

El consentimiento puede ser revocado por cualquier medio y en cualquier momento, pero no tendrá efectos retroactivos. A su vez, dispone que no será necesario el consentimiento, cuando: a) los datos se recaben para el ejercicio de funciones propias de los poderes de la Ciudad de Buenos Aires o en virtud de una obligación legal, b) la información personal se hubieren obtenido de

21 Ley A - N° 1.845. Ciudad Autónoma de Buenos Aires, artículo 6°.

fuentes de acceso público irrestricto, c) se trate de datos personales relativos a la salud y su tratamiento sea necesario por razones de salud pública o emergencia, establecidas por autoridad competente y debidamente fundadas, y d) se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio ²².

La normativa otorga un tratamiento especial a determinado tipo de datos, que son los siguientes:

1) *Datos sensibles*. Establece que ninguna persona será obligada a proporcionar datos sensibles, en particular no podrá solicitarse a ningún individuo como condición para su ingreso o promoción dentro del sector público de la Ciudad de Buenos Aires. Sólo podrán ser tratados estos datos cuando medien razones de interés general autorizadas por ley, o bien con finalidades estadísticas o científicas, siempre y cuando no sean identificados sus titulares.

La ley prohíbe la formación de archivos, registros, bases o banco de datos que almacenen información que directa o indirectamente revele datos sensibles, salvo que una ley expresamente disponga lo contrario o medie el consentimiento libre, previo, expreso, informado y por escrito de su titular.

Datos relativos a antecedentes penales, contravencionales o infracciones administrativas. Esta información sólo puede ser objeto de tratamiento por parte de las autoridades públicas competentes, en el marco de las leyes y reglamentaciones respectivas.

Datos relativos a la salud. La ley les otorga un tratamiento especial aunque conforman un tipo de dato sensible. En tal sentido, dispone que los establecimientos sanitarios dependientes de la Ciudad de Buenos Aires y los profesionales vinculados a las ciencias de la salud que presten servicios en éstos, pueden recolectar y tratar información personal relativa 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 ²³.

22 Ley A - N° 1.845. Ciudad Autónoma de Buenos Aires, artículo 7°.

23 Ley A- N° 1.845. Ciudad Autónoma de Buenos Aires, artículo 9°.

d. *Tipo de acción*

La ley reglamentaria de la acción de protección de datos personales, si bien sigue los lineamientos de la Constitución de la Ciudad ha tenido especialmente en cuenta los parámetros de la ley nacional de habeas data. En efecto, en forma expresa establece que la acción de protección de datos tramitará según las disposiciones de esta ley, y supletoriamente por el procedimiento que corresponda a la acción de amparo ante el Fuero Contencioso Administrativo y Tributario de la CABA y a las disposiciones del Código Procesal Contencioso, Administrativo y Tributario de la Ciudad, relativos al procedimiento sumarísimo ²⁴.

La Ley de Protección de Datos Personales de la CABA fue dictada antes que la ley de amparo de la Ciudad -N° 2.145-, razón por la cual no pudo remitir supletoriamente a tal régimen, en consecuencia, se refirió a la ley procesal más próxima vigente por entonces. En este sentido, PUCCINELLI ²⁵ entiende -con buen criterio- que más allá de la remisión realizada por la ley, dado la falta de norma regulatoria del amparo local, actualmente deben aplicarse supletoriamente las reglas de la ley N° 2.145 por tratarse del marco general del amparo en la Ciudad, y por ser ésta teleológicamente la norma supletoria de la que en definitiva surge la obligación de remisión, contenida en el artículo 16 de la Constitución local.

Este criterio ha sido ratificado recientemente por el Tribunal Superior de Justicia de la Ciudad en el caso “Boero, Dora Patricia c/GCBA”, al señalar que al no estar regulado por la ley N° 1.845 el plazo de interposición del recurso de inconstitucionalidad, corresponde acudir a lo preceptuado en el artículo 22 de la ley N° 2.145 ²⁶.

Esta acción procederá para que los titulares de datos personales tomen conocimiento de la información que a ellos corresponda, que

24 Ley A - N° 1.845. Ciudad Autónoma de Buenos Aires, artículo 30.

25 PUCCINELLI, Oscar R., “La protección de los datos personales y el habeas data en la Ciudad Autónoma de Buenos Aires”, en MARANIELLO, Patricio (dir.), *Constitución de la Ciudad Autónoma de Buenos Aires, Comentada*, La Ley, Ciudad Autónoma de Buenos Aires, 2016, t.1, p. 335.

26 TSJ CABA: “Boero, Dora Patricia c/GCBA y otros s/habeas data s/recurso de inconstitucionalidad concedido”, 20/12/2016.

esté recopilada en bases de datos del sector público de la Ciudad Autónoma de Buenos Aires, su fuente, origen, finalidad o uso que de la misma se haga. En los casos en que se presuma la falsedad, inexactitud, desactualización de la información de que se trata, o el tratamiento de datos se realice en infracción de la ley nacional N° 25.326, podrá exigirse su rectificación, supresión, confidencialidad o actualización²⁷.

Teniendo en cuenta la clasificación referida que hace SAGÜÉS²⁸, podemos decir que la ley reglamentaria de la acción de protección de datos personales de la Ciudad de Buenos Aires establece un habeas data informativo, con sus sub-tipos; habeas data exhibitorio, habeas data finalista y habeas data autoral.

Del mismo modo, prevé para el cumplimiento de los fines mediatos los siguientes tipos; habeas data aditivo, rectificador, reservador y habeas data cancelatorio. Nótese que el artículo 16²⁹ de la ley local es réplica textual del 33 de la ley N° 25.326, por lo que se aplica a este punto lo señalado en el Capítulo 2 punto 3, titulado “tipos de acción”.

27 MINOTTI, Sebastián E., “Nuevas normas de protección de datos personales y privacidad laboral en el ámbito de la Ciudad Autónoma de Buenos Aires”, El Dial, www.eldial.com DC98F.

28 SAGÜÉS, Néstor Pedro, “Subtipos de Habeas Data en el Derecho Argentino...” en *Leyes Reglamentarias de la Reforma Constitucional*. pp. 206-208.

29 Ley A - N° 1.845. Ciudad Autónoma de Buenos Aires, artículo 28.- Procedencia. “*La acción de protección de los datos personales o de habeas data, de conformidad con lo dispuesto por el art. 16 de la Constitución de la Ciudad de Buenos Aires procederá: a) Para tomar conocimiento de los datos personales almacenados en archivos, registros o bancos de datos del sector público de la Ciudad de Buenos Aires, su fuente, origen, finalidad o uso que del mismo se haga. b) En los casos en que se presuma la falsedad, inexactitud, desactualización de la información de que se trata, o el tratamiento de datos en infracción de la Ley Nacional N° 25.326 o la presente ley, para exigir su rectificación, supresión, confidencialidad o actualización. c) En los casos de incumplimiento de las disposiciones previstas en la presente ley. El ejercicio de este derecho no afecta el secreto de la fuente de información periódica. Cuando el pedido de acceso sea relativo a información pública y no a datos personales, será de aplicación la Ley N° 104 de la Ciudad de Buenos Aires*”.

*e. Procedimiento**1) Derecho de acceso y habilitación de la acción*

La ley Dispone que el titular de datos personales, previa acreditación de su identidad, tiene derecho a solicitar y obtener información relativa a los datos referidos a su persona, que se encuentren incluidos en los archivos, registros, bases o bancos de datos del sector público de la Ciudad de Buenos Aires.

En consonancia, el responsable del archivo, registro, base o banco de datos consultado debe proporcionar la información solicitada, sin restricciones ni requisitos de ningún tipo en un plazo no mayor de 10 (diez) días hábiles. El plazo se podrá prorrogar en forma excepcional por otros 10 (diez) días hábiles, de mediar circunstancias que hagan imposible reunir la información solicitada. En su caso, el órgano requerido debe comunicar antes del vencimiento del término, las razones por las cuales hará uso de la prórroga excepcional. Vencido éste sin que se satisfaga el pedido, o si evacuado el informe se estimara insuficiente, quedará expedita la acción de protección de datos personales.

El derecho de acceso sólo puede ser ejercido en forma gratuita y en intervalos no inferiores a dos meses, salvo que se acredite un interés legítimo al efecto, en cuyo caso podrá ejercerse en cualquier momento ³⁰.

2) Derecho de rectificación

Establece que toda persona tiene derecho a que sus datos sean rectificadas, actualizados, y cuando corresponda, suprimidos o sometidos a confidencialidad.

Nuevamente en forma coherente con las prerrogativas establecidas en favor del titular, prevé que el responsable del archivo, registro, base o banco de datos debe proceder a la rectificación, supresión o actualización de los mismos, realizando las operaciones necesarias a tal fin en el plazo máximo de 5 (cinco) días hábiles de recibido el reclamo presentado por el titular de los datos, o una vez advertido el error o falsedad.

El incumplimiento de esta obligación dentro del término acordado en el inciso precedente, habilitará al interesado a promover sin más

30 Ley A - N° 1.845, Ciudad Autónoma de Buenos Aires, artículo 13.

la acción de protección de datos personales prevista. Sin embargo, respecto del derecho de supresión se establece que no procede cuando pudiese causar perjuicios a derechos o intereses legítimos de terceros, o cuando existiera una obligación legal de conservar los datos ³¹.

En el caso, debería interpretarse la frase “perjuicio a terceros” con carácter sumamente restrictivo, dado que no parece una fórmula acertada dejar librada la supresión de un dato personal a lo que pueda o no ocurrir a tercera persona. Justamente, la garantía de habeas data entraña una tutela a los datos personales y no a derechos de terceros ³².

3) *Demanda. Formalidades*

La normativa establece que la demanda debe ser interpuesta por escrito, individualizando el nombre y domicilio del archivo, registro o banco de datos, como también el nombre del responsable y/o encargado y/o usuario del mismo. Deberá igualmente alegar las razones por las cuales entiende que en ese registro o banco de datos existe información referida a su persona.

Por otro lado, el requirente podrá solicitar que mientras dure el procedimiento, el registro asiente que la información cuestionada está sometida a un proceso judicial ³³. Una vez interpuesta la acción, el juez deberá pronunciarse en el término de 3 (tres) días acerca de su admisibilidad formal.

Admitida la acción, a) el juez solicitará al archivo o registro de datos la remisión de la información concerniente al accionante. Podrá solicitar informes sobre el soporte técnico, documentación de base relativa a la recolección, y cualquier otro aspecto que resulte conducente a la resolución de la causa que estime procedente.

b) El archivo o banco de datos tendrá un plazo de 5 (cinco) días hábiles para contestar el informe; no obstante, el plazo podrá ser ampliado prudencialmente por el juez ³⁴.

31 Ley A - N° 1.845, Ciudad Autónoma de Buenos Aires, artículo 13.

32 BASTERRA, Marcela I., *Protección de Datos Personales. Ley 25.326 y Dto. 1558/01 Comentados. Derecho Constitucional Provincial, Iberoamérica y México*, p. 123.

33 Ley A - N° 1.845, Ciudad Autónoma de Buenos Aires, artículo 32.

34 Ley A - N° 1.845, Ciudad Autónoma de Buenos Aires, artículo 33.

c) Una vez que ha sido contestado el informe, el accionante podrá, en el término de 3 (tres) días, ampliar el objeto de la demanda solicitando la supresión, rectificación, confidencialidad o actualización de su información personal. De esta presentación se le dará traslado al demandado, también por el término de 3 (tres) días.

d) Vencido el plazo para la contestación del informe, contestado el mismo o ampliado y contestada la ampliación, el juez procederá a dictar sentencia. La que será comunicada al organismo de control, encargado de llevar un registro al efecto ³⁵.

f. Organismo de control

El título VI de la ley A -N° 1845 regula el órgano de control, disponiendo que será la Defensoría del Pueblo de la Ciudad de Buenos Aires bajo cuya responsabilidad se crea el Registro de datos personales ³⁶.

Igualmente, establece los deberes y facultades que tendrá el organismo, en tanto órgano de contralor establecido en la ley ³⁷, los cuales se condicen claramente con los que le fueron fijados en la Constitución de la Ciudad.

El artículo 137 de la Carta Magna local establece que corresponde a la Defensoría: “(...) *la defensa, protección y promoción de los derechos humanos y demás derechos e intereses individuales, colectivos y difusos tutelados en la Constitución Nacional, las leyes y esta Constitución, frente a los actos, hechos u omisiones de la administración o de prestadores de servicios públicos*”.

Agrega que “(...) *Tiene iniciativa legislativa y legitimación procesal. Puede requerir de las autoridades públicas en todos sus niveles la información necesaria para el mejor ejercicio de sus funciones sin que pueda oponérsele reserva alguna*” y “(...) *vela por la defensa y protección de los derechos y garantías de los habitantes frente a hechos, actos u omisiones de las fuerzas que ejerzan funciones de policía de seguridad local*”.

35 Ley A - N° 1.845, Ciudad Autónoma de Buenos Aires, artículo 37.

36 Ley A - N° 1.845, Ciudad Autónoma de Buenos Aires, artículo 22.

37 Ley A - N° 1.845, Ciudad Autónoma de Buenos Aires, artículos 23 y 24.

Sobre las notas distintivas que caracterizan al Defensor del Pueblo, coincidimos con quienes señalan que debe tratarse de un funcionario independiente, partidario, representante de la Legislatura y con rango constitucional, toda vez que es el encargado de controlar a la Administración. Se ocupa de recibir quejas ciudadanas contra actos lesivos de la Administración pública y/o errores administrativos, con facultades para investigar, criticar y publicitar esas acciones administrativas; como asimismo poseer legitimación procesal para intervenir en juicios ³⁸.

En cierta medida reafirma lo señalado previamente su emplazamiento constitucional dentro del Título Séptimo, del Libro Segundo que lleva por nombre “Órganos de Control”. No obstante y como se observa de la redacción del artículo 137 Constitucional es mucho más que una institución de control. Las funciones de opinión, las tareas de divulgación y la contención comunitaria superan ampliamente la noción de simple contralor.

En consecuencia, podemos afirmar que esta institución ha sido pensada por el constituyente local, como una herramienta imprescindible para llevar a cabo acciones que garanticen los derechos fundamentales que la Constitución porteña de 1996 reconoce, entre los que se encuentran el derecho a la intimidad y la autodeterminación informativa, tutelados por el habeas data ³⁹.

La “Ley Orgánica de la Defensoría del Pueblo de la Ciudad Autónoma de Buenos Aires”, Ley A- N° 3 ⁴⁰, buscó facilitar el acceso a este órgano. En consecuencia, señala que: “*Puede dirigirse al Defensor o Defensora del Pueblo cualquier persona física o jurídica que se considere afectada por los actos, hechos u omisiones previstos en el artículo (...)*” ⁴¹. Agrega que las actuaciones ante el Defensor del Pueblo no están sujetas a formalidad

38 FENTANES, Juan, “Artículo 137. Defensoría del pueblo”, en MARANIELLO, Patricio (Dir.), *Constitución de la Ciudad Autónoma de Buenos Aires, Comentada*, cit., t. 2, p. 1860.

39 AMOR, Alejandro, “La Defensoría del Pueblo”, en BASTERRA, M. (dir.) *Constitución de la Ciudad Autónoma de Buenos Aires, Edición Comentada*, cit., pp.1387 y 1392.

40 Ley A - N° 3, publicada en el B.O.C.B.A. el 27/02/1998.

41 Ley A - N° 3, artículo 25.

alguna, todas son gratuitas para el interesado y no requieren patrocinio letrado ⁴².

Como puede observarse, el legislador porteño optó por dejar el contralor del cumplimiento y aplicación de las leyes N° 1.845 y N° 4.496, en manos de un organismo constituido previamente que tiene amplias facultades para cumplir con esta función.

A nivel nacional se optó por un esquema distinto, a través de la creación de un organismo de control específico dentro del Poder Ejecutivo. La ley N° 25.236 de Protección de Datos Personales dispone en su artículo 29 que: *“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”*. Con esta directiva, el Decreto N° 1.558/01 creó la Dirección Nacional de Protección de Datos Personales, en el ámbito de la Secretaría de Justicia y Asuntos Legislativos del Ministerio de Justicia y Derechos Humanos, como órgano de control de la Ley N° 25.326.

IV. Ley A - N° 4.496 de Identidad real en archivos, registros o bases de datos ⁴³

En el año 2013 se sancionó la ley A - N° 4.496 de *“Identidad real en archivos, registros o bases de datos”*. La norma señala en el artículo 1° que es complementaria de la ley N° 1.845 y que tiene por objeto: *“(…) facilitar la rectificación de los datos personales que se encuentran asentados en registros, archivos o bases de datos públicos o privados dentro de la jurisdicción de la Ciudad Autónoma de Buenos Aires de todas personas que figuran en ellos bajo identidad adulterada, rectificada por resolución judicial o que se han acogido a la normativa vigente de derecho de identidad de género”*.

Al igual que la ley N° 1.845 dispone que la autoridad de aplicación de la misma es la Defensoría del Pueblo de la Ciudad Autónoma de Buenos Aires.

42 Ley A - N° 3, artículos 14 y 26.

43 Ley A - N° 4.496 de la Ciudad Autónoma de Buenos Aires, publicada en el B.O.C.B.A. el 02/05/2013.

En cuanto a la legitimación activa establece que a solicitud de las personas que figuran en registros o archivos públicos o privados, bajo identidad adulterada rectificadas por resolución judicial o que se han acogido a la normativa vigente de derecho de identidad de género, la Autoridad de Aplicación es la encargada de realizar las acciones tendientes a registrar la identidad real y a actualizar los datos asentados. Igualmente, agrega que tal solicitud puede ser revocada en cualquier momento por la persona solicitante.

Por otra parte, prevé que se encuentran obligados a cumplir con la normativa todos los registros o bases de datos públicos o privados obrantes en la Ciudad, incluyendo archivos de historias clínicas, certificados estudiantiles y antecedentes culturales y deportivos, siendo pasibles de las sanciones previstas en la ley N° 1.845 de Protección de Datos Personales y Habeas Data.

V. Decreto N° 725/2007 ⁴⁴

Por medio de este Decreto se aprueba la reglamentación de la ley N° 1.845 de Protección de Datos Personales, reconociendo al titular de los datos los derechos de información, acceso, rectificación, actualización o supresión.

En tal sentido, la reglamentación dispone básicamente que el ejercicio del derecho de acceso no requiere de fórmulas específicas, siempre que se garantice la identificación del titular del dato y/o de sus representantes legales.

Contempla que los responsables de las bases de datos podrán disponer de otros servicios de acceso, como los medios electrónicos, las líneas telefónicas, la recepción del reclamo en pantalla u otro medio idóneo a tal fin.

Finalmente, establece que el órgano requerido deberá comunicar al titular de los datos que ha cumplido con su solicitud, en un término máximo de 5 (cinco) días hábiles contados a partir del vencimiento del plazo para proceder a suprimir, rectificar, actualizar o someter a confidencialidad el reclamo ⁴⁵.

⁴⁴ Decreto N° 725/2007 de la Ciudad Autónoma de Buenos Aires, publicado en el B.O.C.B.A del 24/05/2007.

⁴⁵ Decreto N° 725/2007, Ciudad Autónoma de Buenos Aires. Artículo 13.

VI. Otra normativa actual relevante en la materia

Además de la Constitución local, la ley A - N° 1.845 y el decreto reglamentario N° 725/2007, existen en el ámbito de la Ciudad normas complementarias en la materia.

Siguiendo un criterio cronológico podemos señalar la ley A - N° 712 ⁴⁶ de *“Patrimonio Genético Humano”*, por la que la *“Ciudad garantiza y resguarda el derecho a la dignidad, identidad e integridad de todas las personas con relación a su patrimonio genético”*.

Con posterioridad, en el año 2003 se sanciona la ley H - N° 1.226 ⁴⁷ que crea el *“Sistema de Identificación del Recién Nacido y de su Madre”*, de aplicación obligatoria en todo el ámbito de la Ciudad de Buenos Aires. Este sistema tiene por objeto asegurar a las personas su legítimo derecho a la identidad, así como garantizar la indemnidad del vínculo materno filial.

La ley I - N° 2014 ⁴⁸ del año 2006, crea el *“Registro No Llame”* con el objeto de proteger a los usuarios de servicios telefónicos de los posibles abusos que puedan surgir del uso del telemarketing para publicitar, ofertar, vender y/o regalar bienes y/o servicios.

Por su parte, la Disposición N° 119/2007 ⁴⁹ de la Defensoría del Pueblo de la CABA dispone la creación del *Centro de Protección de Datos de la Ciudad Autónoma de Buenos Aires*.

Esta disposición establece que es responsabilidad primaria del Centro de Protección de Datos: *“Garantizar el cumplimiento de la Ley N° 1845 que tiene por finalidad la protección de las bases de datos personales del Sector Público y en consecuencia la protección del honor, intimidad y autodeterminación infor-*

46 Ley A - N° 712 de la Ciudad Autónoma de Buenos Aires, publicada en el B.O.C.B.A el 17/01/2002.

47 Ley H - N° 1.226 de la Ciudad Autónoma de Buenos Aires, publicada en el B.O.C.B.A el 12/01/2004.

48 Ley I - N° 2.014 de la Ciudad Autónoma de Buenos Aires, publicada en el B.O.C.B.A el 10/08/2006.

49 Disposición N° 119/2007 de la Defensoría del Pueblo de la Ciudad Autónoma de Buenos Aires.

mativa de las personas con motivo del tratamiento de sus datos en la Ciudad de Buenos Aires. Hacer respetar los principios generales y normativos en el tratamiento de datos personales. Velar por los derechos del titular del dato para que pueda acceder, actualizar, rectificar y en su caso suprimir su información personal”.

El mismo organismo sancionó la Disposición N° 89/2008 ⁵⁰ que implementa el Registro de Datos Personales, creado por artículo 23 de la Ley N° 1.845 y reglamentado por el Decreto N° 725/2007.

A través de la Resolución N° 143/2008 ⁵¹ se crea el reglamento para inscribir las bases de datos, en el Registro del Centro de Protección de Datos de la Ciudad de Buenos Aires.

También en 2008 se sancionó la Ley C - N° 2.689 ⁵² que creó la Agencia de Sistemas de Información como una entidad autárquica en el orden administrativo, funcional y financiero, en el ámbito de la Jefatura de Gabinete de Ministros de la Ciudad. Esta normativa dispone que la Agencia de Sistemas será el órgano rector en materia de tecnologías de la información y las comunicaciones en el ámbito del Poder Ejecutivo local, cuya finalidad es organizar y coordinar con todas las dependencias, la infraestructura informática de telecomunicaciones y de los sistemas de información.

Por último, la Resolución N° 177/2013 ⁵³ aprueba el Marco Normativo de Tecnología de la Información, elaborado por la Agencia de Sistemas de Información que deberá ser aplicado en el todo el ámbito del Poder Ejecutivo del Gobierno de la Ciudad Autónoma de Buenos Aires.

⁵⁰ Disposición N° 89/2008 de la Defensoría del Pueblo de la Ciudad Autónoma de Buenos Aires, publicada en el B.O.C.B.A. el 04/07/2008.

⁵¹ Disposición N° 143/2008 de la Defensoría del Pueblo de la Ciudad Autónoma de Buenos Aires, publicada en el B.O.C.B.A. el 15/07/2008.

⁵² Ley C- N° 2.689 de la Ciudad Autónoma de Buenos Aires, publicada en el B.O.C.B.A el 21/05/2008.

⁵³ Resolución N° 177/2013 de la Agencia de Sistemas de Información, publicada en el B.O.C.B.A. el 08/11/2013.

VII. Desafíos actuales de la acción de habeas data

a. *La protección de los datos personales y la responsabilidad de los buscadores de Internet*

En los últimos años, se han dictado en nuestro país numerosas sentencias ⁵⁴ que analizan la posibilidad de solicitar a los buscadores de Internet, la eliminación o el bloqueo de los resultados de ciertos datos personales considerados erróneos, injuriantes o violatorios de la privacidad; así como el alcance de su responsabilidad en estos supuestos.

Dentro de esta jurisprudencia corresponde destacar el fallo de la Corte Suprema de Justicia de la Nación en la causa “Belén Rodríguez” ⁵⁵, en donde el Alto Tribunal advierte el carácter transformador de Internet, en tanto actúa como un medio a través del cual se incrementa la capacidad de los individuos de acceder a la información, fomentando no sólo el pluralismo sino su divulgación. En ese contexto, los buscadores desempeñan un papel preponderante dado que son trascendentales para la difusión global de datos, facilitando el acceso a todo internauta que lleva a cabo una búsqueda a partir del nombre de un determinado sujeto ⁵⁶.

54 A título ejemplificativo pueden mencionarse las siguientes: Cámara Nacional de Apelaciones en lo Civil y Comercial Federal, Sala II: “F. W., .C .G .y otro c/Google Argentina S.R.L s/medidas cautelares”, 17/12/2013; Cámara Nacional de Apelaciones en lo Civil y Comercial Federal, Sala III: “Arte Gráfico Editorial Argentino S.A. c/Castañeda Matías s/cese de uso de marcas/daños y perjuicios”, 11/02/2014; Cámara Nacional de Apelaciones en lo Civil y Comercial Federal, Sala I: “C., R. H. c/Google Inc. y otro s/incidente de apelación de medida cautelar”, 18/03/2014; Cámara Nacional de Apelaciones en lo Civil y Comercial Federal, Sala II: “L., N. L. y otro c/Google Argentina S.R.L s/medidas cautelares”, 31/03/2014; Cámara Nacional de Apelaciones en lo Civil y Comercial Federal, Sala III: “R., L. M. c/Google Inc. s/medidas cautelares”, 29/05/2014; Cámara Nacional de Apelaciones en lo Civil, Sala K: “R., R. c/G. Argentina S.R.L. y Otro s/medidas precautorias”, 30/05/2014; Cámara Nacional de Apelaciones en lo Civil y Comercial Federal, Sala III: “C. E. A. c. Google Inc s/habeas data”, 18/05/2015 y CSJN: “Da Cunha, Virginia c. Yahoo de Argentina S.R.L. y otro s/daños y perjuicios”, 30/12/2014, entre muchas otras.

55 CSJN: “Rodríguez, María Belén c/Google Inc. s/daños y perjuicios”, 28/10/2014.

56 BASTERRA, Marcela I., “La responsabilidad de los motores de búsqueda de Internet en el centro del debate jurídico”, op. cit., p. 145.

PALAZZI⁵⁷ señala con acierto, que actualmente existen buscadores de personas *-personal data agregators-* que permiten aglutinar, relacionar (con sorprendente precisión) y encontrar todo lo que está en la *web* sobre un individuo.

También Ruiz Martínez⁵⁸ se ha pronunciado a favor del derecho a la protección de datos personales y la intimidad en Internet. En este sentido, ha señalado que cuando en la actividad de relacionamiento de datos el buscador proporciona resultados que causan daños al honor o a la intimidad, esa actividad -según las circunstancias del caso- podría estar alcanzada por la Ley Nacional de Protección de Datos Personales. Considera que la persona afectada podrá solicitar a los buscadores el bloqueo del resultado, al entender que el tratamiento de los datos que hace la empresa está alcanzado por la Ley N° 25.326⁵⁹.

La cuestión acerca de si los motores de búsqueda realizan tratamiento de datos, y si corresponde aplicarles la normativa que protege los mismos, fue objeto de análisis a partir del paradigmático fallo “Costeja González”⁶⁰ del Tribunal de Justicia de la Unión Europea.

En este precedente, el Tribunal sostuvo que el gestor o intermediario es responsable del tratamiento de datos desde el momento en que determina la finalidad y los medios de ese tratamiento; de ahí que se lo considere “responsable” en virtud de lo prescripto por el artículo 2º, inciso d) de la Directiva de Protección de Datos de la Unión Europea⁶¹. Agrega, que ya en la sentencia “Lindq-

57 PALAZZI, Pablo A., “El derecho al olvido en internet”, <http://www.rlpdp.com/2012/06/palazzi-el-derecho-al-olvido-en-internet/>

58 Esteban RUIZ MARTÍNEZ expuso su opinión en carácter de orador por la Dirección Nacional de Protección de Datos Personales, en la audiencia pública convocada por la Corte Suprema de la Justicia de la Nación en el caso “Rodríguez, María Belén c/Google Inc s/daños y perjuicios”, del 21/05/2014.

59 Ley N° 25.326, publicada en el Boletín Oficial el 02/11/2000.

60 Tribunal de Justicia de la Unión Europea, Gran Sala: “Google Spain, S.L., y Google Inc. vs. Agencia Española de Protección de Datos (AEPD) y Mario Costeja González”, 13/05/2014.

61 Directiva 95/46/CE de 1995 del Parlamento Europeo y del Consejo Parlamento. Relativa a la protección de las personas físicas en lo que respec-

vist”⁶² había tenido oportunidad de puntualizar que la conducta consistente en hacer referencias en una página *web* a determinada información individual, debe considerarse “tratamiento”.

Con base en estos argumentos, concluyó que toda vez que la actividad de un motor de búsqueda puede afectar derechos fundamentales como la privacidad y la protección de los datos personales, el gestor de ese motor como persona que determina los fines y los medios de la actividad, deberá garantizar el respeto de las exigencias de la Directiva 95/46, a fin de que la tutela consagrada en ésta tenga plena eficacia.

En la misma dirección, apunta que de conformidad con el artículo 6° de la Directiva le corresponde al responsable del tratamiento de datos, asegurar que toda información personal sea tratada de manera lícita y que los datos sean recogidos con fines determinados, explícitos y legítimos, como también que la actividad no se desarrolle de manera incompatible con estos objetivos. Concluye que el responsable debe adoptar todas las medidas razonables para que los datos que no responden a estos requisitos, sean suprimidos o rectificadas.

Entiendo que al momento de decidir si el buscador ha realizado o no el tratamiento de datos personales, deberá aplicarse un criterio sumamente restrictivo en aras de no lesionar la libertad de expresión en Internet.

Aunque no esté consignado en forma explícita, la información de carácter personal -que se encuentra alojada en las diferentes páginas *web* que son indexadas por los buscadores- es susceptible de ser protegida por la garantía del *habeas data* reconocida tanto en la Constitución Nacional como en la local, la Ley N° 25.236 de Protección de Datos Personales y la ley A - N° 1.845 de la CABA.

Comparto el criterio sentado por la Corte en el precedente “Belén Rodríguez”⁶³, en tanto afirma que los motores de búsqueda no tienen responsabilidad objetiva, ni el deber de indemnizar por el simple hecho de la actividad que realizan. Ahora bien, esto no puede

ta al tratamiento de datos personales y a la libre circulación de estos datos. 24/10/1995.

62 C-101/01, EU:C: 2003:596, apartado 25. Citado en el cuerpo de la Sentencia.

63 Caso “Belén Rodríguez”.

llevar a desconocer la posibilidad de los particulares de exigir la supresión, rectificación, confidencialidad o actualización de sus datos personales alojados en las distintas páginas de Internet indexadas por los buscadores ⁶⁴.

b. *Data mining*

Los recursos informáticos permiten la consolidación de información personal proveniente de distintas fuentes, de modo de obtener un conocimiento de la vida de los individuos que no era posible antes de la utilización de los mismos ⁶⁵.

Entre las nuevas técnicas de tratamiento de datos pueden destacarse las que se basan en el cruce de información procedente de distintos bancos o ficheros, para extraer perfiles ya sea con fines comerciales o publicitarios, o para permitir al Estado tener un perfil completo de sus gobernados y orientar la toma de decisiones.

En consecuencia, podemos afirmar que existen grandes intereses detrás del análisis de datos por parte de las empresas y los Estados, siendo uno de los principales objetivos conocer más al consumidor y al ciudadano ⁶⁶.

A la infraestructura de equipos dispuesta para realizar el cruzamiento de datos se la denomina *Data warehouse*, y al tratamiento concreto que se efectúa con los datos *Data mining* o “minería de datos”. La propia denominación nos permite descubrir su finalidad, que no es otra que indagar en distintas bases de información en las que las personas consintieron su tratamiento, con el objeto de obtener a su vez, una nueva base de datos como resultante del entrecruzamiento de las anteriores ⁶⁷.

64 BASTERRA, Marcela I., “La protección de datos personales frente a las nuevas tecnologías”, *Microjuris*, Ciudad Autónoma de Buenos Aires, 2 de septiembre de 2016.

65 RODRÍGUEZ VILLAR, Pacífico, “La protección de datos personales y la esfera de actuación de las autoridades de control”, en *Régimen jurídico de los datos personales*, t.1, p. 187.

66 BRITOS Cristina, “Reflexiones en torno a dos extraños invisibles: el cloud computing y big data”, *El Dial*, www.eldial.com, DC1BC9.

67 BASTERRA, Marcela I., “Datos personales para fines publicitarios. A propósito de la Disposición 4/2009 de la DNPDP”. op. cit., p. 1.

En general los tratamientos de *data mining* se efectúan en sistemas informáticos distintos a los del resto de la empresa o el Estado, incluyendo en los mismos los datos procedentes del resto de los ficheros para su interrelación (*data warehouse*)⁶⁸. Estas prácticas en algunos casos dan lugar a conductas al margen de la normativa sobre protección de datos personales, de allí los recaudos que se deben tomar.

En principio, salvo las excepciones del art. 7° de la ley A - N° 1.845 (datos que no requieren del consentimiento) y en la medida que no resulten directa o indirectamente en el tratamiento de datos sensibles, según los arts. 3° y 8° la ley, se puede realizar cualquier técnica de *data mining* si existe el consentimiento previo del sujeto titular del dato. El hecho de haber prestado el consentimiento para la utilización de información personal en otros casos, no significa que se pueda efectuar un tratamiento paralelo dado que supondría la vulneración del principio de finalidad contenido en el artículo 6° de la ley local.

Los titulares de los datos en algunos casos no comprenden que su información puede ser combinada con otros datos de perfil existentes, de manera que revele aspectos íntimos, y normalmente carecen de una íntegra comprensión de las interpretaciones, inferencias y/o deducciones que se pueden extraer de sus datos combinados con técnicas de *data mining* o análisis⁶⁹.

Actualmente, la metodología de *data mining* ha logrado un gran impulso con la llegada y evolución de la red. La cantidad de datos de un usuario que puede combinar un portal de comercio electrónico del Estado es inmensa, partiendo de los datos voluntariamente introducidos por el usuario registrado, a los hábitos de navegación que demuestre en su utilización diaria de los servicios de la *web*.

Sin embargo, no todos los portales informan de la existencia de ficheros de *data mining* y de la finalidad del tratamiento que efectúan con los datos de los registrados. Esta situación en principio, constituiría una violación a la ley A - N° 1.845 en los puntos referi-

68 Ver de ÁLVAREZ CIVANTOS, Oscar J., *Normas para la implementación de una eficaz protección de datos de carácter personal en empresas y entidades*, Comares, Granada, España, 2002, p. 73/75.

69 GRANERO, Horacio R., "Internet de las cosas, luces y sombras", *El Dial* 18/11/2015, elDial DC2039.

dos. Para que así no fuera, deberá tratarse de casos en los que sea notorio que se busca sólo formar perfiles con miras a ofrecer un servicio, del que se infiera claramente que no es posible su utilización con finalidad discriminatoria alguna.

Igualmente, cuando una empresa o el Estado lleve a cabo el cruce de datos deberá notificar el resultado a su titular, y en caso de no contar con el consentimiento o si éste fuera revocado, automáticamente sacar el dato del correspondiente registro.

También pesa sobre el titular del registro la adopción de medidas técnicas y organizativas aplicables a los mecanismos de disociación de datos, que resulten necesarias para garantizar la seguridad y confidencialidad de los mismos.

c. *Cloud computing*

El “*cloud computing*” -“computación en la nube” o “servicios en la nube”- ha sido definido por el NIST (Instituto Nacional de Estándares y Tecnología Estadounidense) como “Un modelo que permite el acceso bajo demanda a través de la red a un conjunto compartido de recursos de computación configurables (como por ejemplo red, servidores, almacenamiento, aplicaciones y servicios) que pueden ser rápidamente aprovisionados con el mínimo esfuerzo de gestión o interacción del proveedor de servicio”⁷⁰.

Esta nueva tecnología permite tener archivos, información y aplicaciones informáticas en Internet pudiendo acceder a ellos desde cualquier computadora, sin necesidad de tenerla almacenada en un espacio propio. Todo ese contenido “en la nube” está compuesto por “datos personales”.

En consecuencia, la posibilidad de tratamiento de datos fuera del territorio de la Ciudad Autónoma de Buenos Aires e incluso del territorio nacional, es una característica propia del *Cloud Computing* y constituye un elemento de especial relevancia que debe tenerse en cuenta, en la medida en que no puede ejercerse un control completo del tratamiento de los mismos.

70 Instituto Nacional de Estándares y Tecnología Estadounidense, “*The NIST definition of Cloud Computing*”, en <http://csrc.nist.gov/publications/nits-pubs/800-145/SP-800-148.PDF>, traducido por, BRITOS, Cristina, “Reflexiones en torno a dos extraños invisibles: el cloud computing y big data”, El Dial, www.eldial.com, DC1BC9.

Actualmente en Argentina no existe una regulación específica para la “computación en la nube”, pero coincido ⁷¹ en que el contenido de ésta se compone de “datos personales”, por lo tanto, la normativa sobre la materia le resulta aplicable.

En este sentido, los servicios en la nube constituyen un tratamiento informatizado de datos personales por cuenta de terceros en los términos del artículo 3° de la ley A - N° 1.845, que define al tratamiento de datos como: *“Cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, registro, organización, elaboración, extracción, utilización, cotejo, supresión, y en general, el procesamiento de datos personales, así como también su cesión a terceros a través de todo tipo de comunicación, consulta, interconexión, transferencia, difusión, o cualquier otro medio que permita el acceso a los mismos”*.

Sin embargo, la Ciudad ha sido pionera en la materia dado que en enero de este año por Resolución N° 12/2017 ⁷² aprobó el “Marco Normativo del Cloud Computing”, al cual deberán atenerse todos los organismos centralizados y descentralizados del Poder Ejecutivo local que tengan interés en llevar a cabo un proyecto a implementarse en el “cloud”.

El objetivo de esta normativa es establecer los criterios que se deben considerar para proteger la información del Gobierno de la Ciudad, seleccionando el escenario más acorde de acuerdo al tipo de información que se desea publicar. De igual forma, la norma agrega que el tratamiento de datos personales se sujetará a las medidas de seguridad establecidas en el artículo 17 de la Ley A - N° 1845.

VIII. Conclusiones

Las garantías no son otra cosa que las técnicas previstas por el ordenamiento para reducir la distancia estructural entre normati-

71 Ver FRENE, Lisandro, “Privacidad en los ‘servicios informáticos en la nube’”, en *Régimen jurídico de los datos personales*, p. 699. AAVV, *Protección de datos y habeas data: una visión desde Iberoamérica*, Agencia Española de Protección de Datos, Madrid, España, 2015, p. 10.

72 Resolución N° 12/2017 de la Agencia de Sistemas de Información de la Ciudad Autónoma de Buenos Aires, publicada en el B.O.C.B.A. el 01/02/2017.

vidad y efectividad; por lo tanto, para posibilitar la máxima eficacia de los derechos fundamentales en coherencia con su estipulación constitucional ⁷³.

La protección de los individuos frente al uso abusivo de la informática, que violenta derechos fundamentales como la intimidad, el honor, la imagen, etc., es uno de los objetivos fundamentales que tuvo en miras el constituyente de la Ciudad al establecer esta herramienta.

La intimidad es un aspecto de la personalidad exento del conocimiento por parte de los demás, que se materializa en el derecho de cada individuo a que otras personas no tengan información documentada, que éste no quiere que sea ampliamente conocida.

Es entonces un derecho personalísimo, entendido como aquellas prerrogativas de contenido extra-patrimonial, inalienables, perpetuas y oponibles *erga omnes*, que corresponden a toda persona por su sola condición de tal desde antes de su nacimiento y hasta después de su muerte, y de las que no puede ser privado por la acción del Estado ni de otros particulares, porque ello implicaría desmedro o menoscabo de la personalidad.

Nuestro país no escapa a la tendencia imperante hacia nuevas propuestas legislativas, que a través de reformas a las leyes de protección de datos o mediante la presentación de proyectos específicos, están incorporando un nivel más avanzado de resguardo legal respecto de los derechos de los titulares de la información.

En este sentido, entiendo conveniente reformular y actualizar las leyes que regulan la protección de datos personales en Argentina y en la Ciudad de Buenos Aires, a fin de lograr un marco jurídico que pueda acompañar y dar respuestas adecuadas a las lagunas que plantean las nuevas tecnologías. Por otra parte, el carácter transfronterizo de Internet, implica un desafío aun mayor en la materia.

Lo señalado previamente no implica limitar el desarrollo de Internet y demás herramientas tecnológicas, o poner limitaciones a la transferencia de información, sino buscar una regulación razonable que proteja a los usuarios de Internet y los titulares de datos personales, garantizando su privacidad y titularidad.

73 FERRAJOLI, Luigi, *Derechos y Garantías. La Ley del más débil*, Trotta, Madrid, España, 2004, p. 35.