La Garantía Constitucional de Habeas Data.

Lineamientos Generales de la Ley de Protección de Datos Personales.

Marcela I. Basterra

Sumario: 1. Introducción. 2. Principales lineamientos de la Ley Nacional de Protección de Datos Personales. a. Principios generales. a.1. Objeto de la Ley. a.2. Excepciones al derecho de acceso. a.3. Definiciones. a.4. El núcleo o los principios de la ley; Licitud, Calidad y Consentimiento expreso en materia de datos personales. b. Derechos de los titulares. b.1. Derecho de acceso. b.2. Derechos de rectificación, supresión, actualización y confidencialidad. c. El Órgano de Control. 3. Conclusiones.

1. Introducción.

América Latina se inserta en la realidad informática a través de normas sobre protección de datos personales de una manera ciertamente peculiar. Inicialmente, no se verificó la sanción de normas generales o sectoriales como en Europa o Estados Unidos; sino que, su inserción se realizó directamente en las Constituciones reformadas con posterioridad al proceso de recuperación democrática en la mayoría de los países de la región, iniciado a partir del año 1980.

En ese contexto, los constituyentes siguieron fundamentalmente la tendencia fijada por las Constituciones de Portugal y España, estableciendo reglas breves y genéricas sobre protección de datos personales. A continuación de la reforma de la Constitución brasileña de 1988, comienza un movimiento en Latinoamérica, decididamente con la intención de incorporar una acción específica, de garantía de los derechos que pudieran vulnerarse a través del tratamiento de datos personales.

La Constitución del Brasil de 1988 será la que regulará por primera vez la garantía específica, denominándola *"habeas data"*1***[1]***.* Sin embargo, curiosamente, no establece los principios relativos al tratamiento de datos personales específicamente, ni reconoce un derecho al control o autodeterminación de los mismos.

Tres años más tarde, la Constitución colombiana de 1991 asumió la problemática, e incorporó reglas relativas al tratamiento de datos personales, aunque no siguió el

---

1[1] Constitución de Brasil, artículo 5 inc. LXXII: *"Se concederá habeas data: a) para asegurar el conocimiento de informaciones relativas a la persona del impetrante, que consten en registros o bancos de datos de entidades gubernamentales o de carácter público; b) para rectificar datos, cuando no se prefiriera hacerlo por procedimiento secreto, judicial o administrativo".*

esquema brasileño, estableciendo un derecho concreto sobre la información personal, protegido a través de la acción de tutela2[2].

En 1992 lo hizo la Constitución paraguaya3[3] y, en 1993, la Constitución peruana tratará en forma más adecuada la cuestión, toda vez que define; por un lado, el contenido del derecho a la protección de los datos personales y, por el otro, crea una garantía específica tendiente a la tutela efectiva de los mismos4[4].

En 1994 con la reforma constitucional argentina; el habeas data, era una de las garantías que, sin duda, no podía quedar excluida. Así es incorporada, aunque sin ser rotulada con ese nombre; como acción y como subtipo de amparo en el artículo 43, 3° párrafo, seguidamente a la regulación, en los dos primeros párrafos de las acciones de amparo individual y amparo colectivo, respectivamente.

A partir de la década del ’90 y del año 2000 se sancionaron sucesivas leyes en la región, complementarias de las normas constitucionales, estableciendo a la acción de habeas data como un proceso especial o autónomo, regido por cada ley en cuestión. Tal el caso de Brasil en el año 1997 con la sanción de la Ley 9.5075[5]; Portugal con la Ley 676[6],de 1998; Chile en 1999 a través de la Ley 19.6287[7] y, España por medio

---

2[2] Constitución de Colombia, artículo 15: *“Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de los datos se respetarán la libertad y demás garantías consagradas en la Constitución”*.

3[3] Constitución de Paraguay, artículo 135: *“Toda persona puede acceder a la información y a los datos que sobre sí misma, o sobre sus bienes, obren en registros oficiales o privados de carácter público, así como conocer el uso que se haga de los mismos y de su finalidad. Podrá solicitar ante el magistrado competente la actualización, rectificación o la destrucción de aquéllos, si fuesen erróneos o afectaran ilegítimamente sus derechos”*.

4[4] Constitución de Perú, artículo 2: *“Toda persona tiene derecho (…) 5. A solicitar sin expresión de causa la información que requiera y a recibirla de cualquier entidad pública, en el plazo legal, con el costo que suponga su pedido. Se exceptúan las informaciones que afectan la intimidad personal y las que expresamente se excluyan por ley o por razones de seguridad nacional. (...)* 6. *A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal o familiar. 7. Al honor y a la buena reputación, a la intimidad personal y familiar así como a la voz y a la imagen propias* (...)”. Artículo 200 *“Son garantías constitucionales: (...) 3) La acción de habeas data, que procede contra el hecho u omisión por parte de cualquier autoridad, funcionario o persona, que vulnera o amenaza los derechos a que se refiere el artículo 2º, inciso 5º y 6º, de la Constitución”.*

5[5] Ley 9.507 de Brasil, publicada en el BO del 12/11/1997.

6[6] Ley 67/1998 de Portugal, publicada en el DR Nº 247 (Serie I - A), del 26/10/1998.

7[7] Ley 19.628 de Chile, publicada en el BO del 28/08/1999.

de la *"Ley Orgánica de Regulación del Tratamiento Automatizado de datos"* (LORTAD) Nº 5/19928[8], reformada en 1999 por la Ley 159[9].

En el nuevo siglo, Argentina sanciona la Ley 25.326[10][10] en el año 2000; Paraguay en 2001 sigue el camino con la Ley 1.682[11][11]; Perú, en 2001 a través de la Ley 27.489[12][12] y, Colombia en el año 2007, con la sanción de la Ley 221[13][13].

En el presente trabajo, intentaré analizar los principales lineamientos que se encuentran plasmados en la Ley Nacional de *"Protección de Datos Personales*", Nº 25.326.

2. Principales lineamientos de la Ley Nacional de Protección de Datos Personales.

La ley de protección de datos personales (en adelante LPDP) consta de siete capítulos. Con la finalidad de lograr una sistematización -sin que la ley lo establezca- considero, que se advierten en la normativa, tres fases claramente diferenciales: a) La primera fase, que regula los principios relativos al tratamiento de datos personales (artículos 1º a 7º); b) La segunda fase, que se refiere concretamente a los derechos de los titulares de los datos personales (artículos 14 y 16), que he denominado "de eficiencia", ya que, con razón, establece una instancia pre-judicial y, por último c) La tercera fase, reglamentaria de las herramientas tendientes a efectivizar los principios antes descriptos (artículos 21, 29, 31 y 32)14[14].

a. Principios generales.

Los artículos 1º a 7º de la ley 25.326 regulan los denominados "principios generales" sobre el tratamiento de los datos personales.

a. 1. Objeto de la Ley.

8[8] Ley 5/1992 (LORTAD). España, publicada en el BOE N° 262, del 31/10/1992.

9[9] Ley 15/1999 de España, publicada en el BOE Nº 298 del 14/12/1999.

10[10] Ley 25.326 de Argentina, publicada en el BO del 02/11/2000.

11[11] Ley 1.682 de Paraguay, publicada en el BO del 16/01/2001.

12[12] Ley 27.489. Perú, publicada en el BO del 28/06/2001.

13[13] Ley 221/2007. Colombia, publicada en el BO del 04/06/2007.

14[14] Véase de BASTERRA, Marcela I., Protección de datos personales. Ley 25.326 y Dto 1558/01. Comentados. Derecho Constitucional Provincial. Iberoamérica y México, Editorial Ediar y UNAM, Buenos Aires- México, 2008, p. 195/199.

La norma al establece el objeto, en el artículo 1º, cuando dispone *"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".*

Sin perjuicio de que el legislador se aparta de la norma constitucional, en tanto aquélla no menciona expresamente los derechos tutelados por la garantía, y el articulado de la norma sí lo hace, tal como lo he sostenido[15][15], toma únicamente el derecho a la intimidad y al honor, aún cuando la Constitución implícitamente, protege el derecho a la intimidad informática, que implica la posibilidad de ejercer la autodeterminación informativa y, a través de ella, la protección del derecho a la imagen o el propio perfil.

La ley, está orientada a la protección integral 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.

En este orden de ideas, no resulta aplicable a otros registros de información que tienen distintas finalidades, por ejemplo los registros periodísticos que se mantienen dentro de un ámbito de estricto secreto, por imperio de la propia Constitución y la ley. Puede asegurase que guarda total coherencia con el bien jurídico que se pretende tutelar -la intimidad de los datos personales-. Si así no fuera, con el fin de proteger el derecho a la intimidad, estaríamos, a su vez, vulnerando el mismo derecho, tal el caso si se permitiera el acceso a registros privados *"que sean de uso estrictamente personal o profesional".*

Sancionada la ley, igualmente, no resultaba suficiente la previsión de referirse a la posibilidad de acceso y rectificación, únicamente de aquellos bancos de datos *"privados destinados a proveer informes"*. En efecto, existen numerosos archivos de datos privados que no tienen por finalidad proveer informes pero que, por la actividad propia que realizan, vuelcan una gran cantidad de información en registros informatizados; tal el caso, de las personas jurídicas con múltiples integrantes, como las Universidades, Colegios Profesionales, Obras Sociales -entre otros-.

En estos casos, es necesario establecer si se trata de información propia de la entidad, o si en realidad son datos para utilización de sus integrantes o asociados; por lo que el artículo 1° del Decreto 1558/0116[16], viene a subsanar y complementar la omisión legal, disponiendo que; "*quedan excluidos de la ley únicamente aquellos archivos de datos privados para un uso exclusivamente personal*".

Por consiguiente, se entienden incluidas en el concepto de *"bancos de datos destinados a proveer informes"* otras entidades, tales como las referidas y, los

---

15[15] BASTERRA, Marcela I., La garantía constitucional del habeas data. En AAVV: Derecho Procesal Constitucional MANILI, Pablo L; Coordinador; Editorial Universidad, Buenos Aires, 2005, p.141/186.

16[16] Decreto 1558/01. Publicado en el BO el 03/12/2001.

establecimientos educativos, clubes deportivos, etc. Los que, si bien no están específicamente destinadas a proveer informes, su trabajo se realiza recopilando datos en forma permanente, por lo que se encuentran excluidos de cumplir con la normativa de referencia. Justamente, el decreto 1558/01 establece *"a los efectos de esta reglamentación, quedan comprendidos en el concepto de archivos, registros, bases o bancos de datos privados destinados a dar informes, aquellos que exceden el uso exclusivamente personal y los que tienen como finalidad la cesión o transferencia de datos personales, independientemente de que la circulación del informe o la información producida sea a título oneroso o gratuito"*[17][17].

a. 2. Excepciones al derecho de acceso.

El acceso a los datos personales, como todo principio general, tiene ciertas excepciones que se encuentran contempladas en el artículo 17[18][18], de la ley reglamentaria en tanto establece que los responsables o usuarios de bancos de datos públicos, pueden denegar el acceso, la rectificación o supresión, siempre que medie una decisión fundada, en aras de; a) la protección de la defensa de la Nación, b) del orden y la seguridad pública y, c) de la protección de los derechos de terceros.

Asimismo, la norma prevé la denegación de la información, cuando se pudieran obstaculizar; a) actuaciones judiciales o administrativas en curso vinculadas a la investigación; b) funciones de control de la salud y medio ambiente; c) la investigación de delitos penales y, d) la verificación de infracciones administrativas.

Por último, establece que la resolución que así lo disponga debe ser fundada y notificada al afectado. No obstante, el acceso a los registros en cuestión, debe permitirse, siempre -sin excepción- en oportunidad en que el afectado tenga que ejercer su derecho de defensa.

En tal sentido, cuando los derechos de acceso y tratamiento de datos personales, colisiona con un bien de interés público orientado a la protección de toda la comunidad; como la seguridad y defensa estatal, aquéllos deben ceder en aras de la salvaguarda y preservación del interés general.

17[17] Decreto 1558/2001, artículo 1°.

18[18] Ley 25.326, 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".*

Sin embargo, a pesar de la excepción impuesta por el legislador, la protección de la defensa de la Nación no puede cercenar de modo arbitrario la garantía constitucional del acceso a los datos personales. Sólo en determinados supuestos, el responsable del banco de datos públicos puede denegar los derechos acordados a los titulares, por lo que, tratándose de una excepción, deberá ser interpretada con carácter sumamente restrictivo. Ello es así además, porque surge con claridad la exigencia legal de la existencia de resolución fundada; lo que implica que nunca podrá denegarse un derecho al titular, por la simple invocación de la prerrogativa del artículo 17 de la LPDP19[19].

Ningún individuo medianamente informado, duda de la conveniencia de una zona de reserva estatal, dado que se trata de una necesidad históricamente probada de la que depende, muchas veces, la supervivencia y estabilidad del sistema político[20][20]. No obstante, tal circunstancia debe ser invocada por el responsable del archivo o banco de datos públicos y, la denegatoria debe realizarse en los términos estrictos que la propia ley establece.

a. 3. Definiciones.

Resulta importante el artículo 2° toda vez que, en el mismo están contenidas las definiciones y el significado de los conceptos que se manejarán en toda la norma, de modo detallado y preciso. Por consiguiente, esta previsión, no amerita aclaración alguna. En efecto, la relevancia de la pormenorización de conceptos reside en que es, en principio, una técnica legislativa inadecuada e imperfecta, la de incorporar definiciones en una ley.

En contrario, se convierte en muy buena técnica cuando se trata de un tema sumamente específico[21][21] como el de este caso, dado que es imposible interpretar la

---

19[19] Puede mencionarse el caso *"Ganora" (CSJN, Fallos 322:2139)* donde la Corte Suprema de Justicia de la Nación sostuvo que *"en principio, la obtención de información sobre datos personales obrantes en los organismos y fuerzas de seguridad halla adecuación legal en la acción de hábeas data ello sin perjuicio de que el suministro de esa información pueda, eventualmente afectar la seguridad, la defensa nacional, las relaciones exteriores o una investigación criminal, cuestión que en cada caso deberá ser invocada por el titular de la respectiva institución. Al ser ello así, la decisión del a quo de rechazar la acción por considerar que los particulares no pueden tener acceso a la obrante en las fuerzas armadas y organismos de seguridad del Estado "por obvias razones de seguridad pública" constituye una afirmación dogmática carente de razonabilidad, pues el no haberse librado los oficios requeridos, no existe la respuesta pertinente del titular de la institución que haga saber si obra la información requerida y si existen las razones que, en definitiva, pudieran impedir al legitimado acceder a ella".*

20[20] FERNÁNDEZ ALLES, "Los secretos de Estado en España: jurisprudencia y teoría constitucional", La ley 1999-2, citado por DELGADO GIL, Andrés, "El delito de revelación de Secretos de Estado en los artículos 598 CP común y 53 CP militar", reflexiones sobre sus diferencias", Revista Electrónica de Ciencia penal y Criminología, 13/7/2005. www.criminet.urg.es

21[21] Véase 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.

ley, sin conocer el significado de algunos temas muy puntuales. Sirva como ejemplo la frase **"***disociación de datos"*22[22]**,** que es utilizada en repetidas oportunidades por el legislador.

a. 4. El núcleo o los principios de la ley; Licitud, Calidad y Consentimiento expreso en materia de datos personales.

El artículo 3º de la LPDP, se refiere a la **licitud de los archivos de datos** cuando la formación de éstos se encuentren debidamente inscriptos, de acuerdo a las propias disposiciones de la ley y, a las demás leyes que se dicten en su consecuencia.

La condición de la inscripción para la licitud en la formación de archivos de datos, sólo es exigible cuando se trate de ficheros de datos de carácter personal, esto es, asociados o vinculados a personas determinadas o determinables. Igualmente se requiere que las operaciones y procedimientos realizados para el tratamiento de los datos del archivo, se ajusten a los principios establecidos por la misma ley a los efectos de mantener en el marco de la licitud a aquéllos[23][23].

Básicamente cuando la normativa se refiere a este requisito de "licitud" del artículo 3**°,** sin duda, lo hace teniendo en cuenta la obligación legal que se refiere al Registro en que deben inscribirse las bases de datos, tanto públicas como privadas. Esto es que, es lícita la recolección de datos, además si el Banco o Archivo de datos, se inscribió en el Registro, cumpliendo los requisitos del artículo 21 que son, como mínimo, los siguientes: a) Nombre y domicilio del responsable, b) Características y finalidad del archivo, c) Naturaleza de los datos personales contenidos en cada archivo, d) Forma de recolección y actualización de datos, e) Destino de los datos y personas físicas o de existencia ideal a las que pueden ser transmitidos, f) Modo de interrelacionar la información registrada, g) Medios utilizados para garantizar la seguridad de los datos, debiendo detallar la categoría de personas con acceso al tratamiento de la información, h) Tiempo de conservación de los datos, por último, i) Forma y condiciones en que las personas pueden acceder a los datos referidos a ellas y los procedimientos a realizar para la rectificación o actualización de los datos.

La sujeción a la finalidad del registro o base de datos es un principio esencial, toda vez que requiere que los datos recogidos sean adecuados en orden a una finalidad o propósito predeterminado al crearse el archivo, el cual se identifica con el interés legítimo de quien recolecta los datos para su tratamiento. La legitimidad del fin para el cual ha sido creado el registro es el fundamento que justifica el uso de datos

22[22] Ley 25.326, artículo 2°: *"(…) Disociación de datos: Todo tratamiento de datos personales de manera que la información obtenida no pueda asociarse a persona determinada o determinable".*

23[23] PEYRANO, Guillermo F., Régimen Legal de los Datos Personales y Hábeas Data. Comentario a la ley 25.326 y a la reglamentación aprobada por Dec. 1558/2001, Lexis Nexis, Depalma, Buenos Aires, 2002, p. 66.

personales de terceros y a su vez establece un límite para la utilización de los mismos[24][24].

El artículo 4° se refiere a la **calidad de los datos**, mencionando expresamente el deber de los responsables de recopilar y dar tratamiento sólo a aquellos datos *"veraces y actualizados",* estableciendo que "*aquellos datos que sean total o parcialmente inexactos o sean incompletos deben ser suprimidos o completados por el responsable".*

Constituyen el principio de la calidad de los datos, un complejo de obligaciones estatuidas por la ley, que inciden sobre los involucrados en los distintos aspectos del "tratamiento" de los datos personales; obligaciones éstas enderezadas a preservar tanto condiciones de los datos considerados en sí mismos, como derechos de los titulares de esas informaciones reconocidos por la misma norma. La finalidad, es comprometer a los responsables de estos ficheros, bancos, bases o archivos, a adoptar los recaudos necesarios para que la información que vayan almacenando en los mismos, responda a exigencias tales como exactitud, veracidad, pertinencia, actualidad, etc. Así como serán objeto de consideración, tanto los medios como las finalidades con que dichos datos son obtenidos y archivados.

El **consentimiento** exigido por el artículo 5º25[25], resulta ser un elemento radical. Justamente, todos los bancos que deseen tratar datos de personas físicas o jurídicas, como regla general deben requerir, de modo previo el consentimiento para el tratamiento de los mismos, salvo que los datos se encuentren en alguno de los supuestos legales que eximen del mismo26[26].

24[24] GILS CARBÓ, Alejandra M. Régimen legal de las bases de datos y habeas data. Ed La Ley. Buenos Aires, 2001, p. 74.

25[25] Ley 25.326, artículo 5°: "*(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 6° 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".*

26[26] BASTERRA Marcela, "El consentimiento del afectado en el proceso de tratamiento de datos personales" JA -Lexis Nexis-. Número Especial, 28 de Abril de 2004, p. 6.

Por consiguiente, la normativa exige que el consentimiento sea libre, refiriéndose, claramente, a los principios generales del derecho. Como todo acto voluntario, el mismo debe configurarse con los elementos determinantes de validez; discernimiento, intención y libertad -artículo 897 del Código Civil-. Como contrapartida, el consentimiento se verá afectado por las mismas causales que en los casos de los actos voluntarios, tales como la inmadurez, la alteración de las facultades mentales, el dolo, el error y la violencia.

Entonces, cuando la ley establece este segundo requisito es claro que tuvo en miras el carácter "expreso" del consentimiento que contempla el Código Civil en su artículo 917 –verbalmente, por escrito o por signos inequívocos- sólo que en este caso particular es notorio que la ley LPDP privilegia el consentimiento por escrito.

Sin embargo, al no surgir prohibición alguna de aceptar el consentimiento verbal y, en consonancia con el artículo 15 de la LPDP, no habría dudas, en principio en aceptar el consentimiento en forma oral, por teléfono, por Internet, etc. Sin embargo, sólo tendría validez si se puede demostrar fehaciente e inequívocamente que dicho consentimiento fue otorgado.

Por otro lado, las excepciones están taxativamente establecidas -ver nota al pié N° 25- por lo que, aunque a veces resulte antipático y hasta molesto, no se requerirá consentimiento alguno, cuando los datos se refieran a casos específicos exceptuados por la LPDP; tales como el nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento o domicilio. Tampoco si se refieren a los datos crediticios, siempre que éstos sean pasivos, o sea, deudas y que cumplan con el requisito de calidad; es decir, que sean ciertos, veraces y adecuados; éstos, son sólo algunos de los ejemplos más habituales.

En síntesis, el consentimiento es una declaración de voluntad del titular del dato, de la que en forma inequívoca se infiera que el mismo ha autorizado al tratamiento de un dato personal.

El artículo 6º LPDP prevé que cuando los datos personales se recaben, previamente se debe informar a los titulares en forma expresa y clara; la finalidad de la recopilación de los mismos, el carácter facultativo u obligatorio de dar esos datos, los derechos de los titulares, etc. Al respecto, se ha señalado que el supuesto al que sujeta el cumplimiento de este deber, abarca una sola de las posibles modalidades de obtención de este tipo de informaciones; que es la correspondiente a la obtención de datos en forma directa de su titular[27][27] con lo que se limita la operatividad de la exigencia a esta circunstancia. Esta obligación forma parte del derecho a controlar sus datos por parte de sus titulares, y consiste, además, en tomar conocimiento de la existencia del almacenamiento de datos, el propósito de los mismos, la identidad y residencia de su titular o responsable.

Por último, en lo que hace a los principios generales, el artículo 7º LPDP reglamenta los aspectos relativos a los datos sensibles, que son aquellos que revelan origen racial

27[27] PADILLA, Miguel M, Banco de datos y acción de Habeas Data, Editorial Abeledo Perrot, Buenos Aires, 2001, p.158.

y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual28[28].

Al efecto establece que *"ninguna persona puede ser obligada a proporcionar datos sensibles"*, lo que no significa que esté prohibido proporcionarlos si el propio titular del dato por sí mismo quisiera hacerlo. Así, de la norma se infieren dos reglas básicas en materia de tratamiento de los datos sensibles: a) por un lado, que no hay obligación de proporcionarlos; y b) por el otro, que sólo pueden ser recolectados y tratados por razones de interés general autorizadas por la ley.

Sin embargo, la recolección de estos datos puede efectuarse para fines estadísticos y científicos sin que medie la identificación de los titulares, en cuyo caso el dato se despersonaliza y pasa a ser un dato anónimo, ajeno a la protección especial que los mismos merecen.

En otros supuestos algunos datos sensibles, pueden ser recolectados mediante una autorización legal; tal es el caso de la Iglesia Católica, las Asociaciones religiosas y las Organizaciones políticas y sindicales que pueden llevar un registro de sus miembros, aun cuando, como regla general esté prohibida la formación de bases que almacenen datos sensibles29[29].

b. Derechos de los titulares.

b.1. Derecho de acceso.

El acceso a los datos personales debe llevarse a cabo, conforme lo establece la ley, de acuerdo a algunas formalidades previstas en los artículos 14 y 16.

En primer lugar, la ley reconoce al titular de los datos, o a quienes estuvieran legitimados en virtud del artículo 34 -con el único requisito de acreditar su identidad- la posibilidad de acceder a los bancos de datos públicos o privados destinados a proveer informes, para conocer los datos personales que de él consten en una base o registro.

Ante la requisitoria, el responsable del banco de datos fehacientemente intimado, debe proporcionar la información solicitada dentro de los diez días, en caso contrario o que el informe sea insuficiente -a criterio del titular del dato-; quedará expedita la acción de habeas data.

La norma contempla la posibilidad de interponer la acción una vez intentada la vía directa ante el banco de datos público o privado a que se refiere la ley. Esto es, la ley habilita una instancia “prejudicial”; antes de concurrir en forma directa a solicitar la jurisdicción.

b. 2. Derechos de rectificación, supresión, actualización y confidencialidad.

28[28] Ley 25.326, artículo 2°.

29[29] BASTERRA, Marcela I., “Protección de datos personales. Ley 25.326 y Dto 1558/01. Comentados…“ Op. Cit. p. 391/401

Una vez que el titular o sus sucesores acceden al dato personal, según lo que corresponda, y en los términos del artículo 16, pueden solicitar que los mismos sean rectificados, actualizados, suprimidos o se establezca confidencialidad en torno al dato; en el plazo máximo de cinco días hábiles de recibido el reclamo del titular de los datos o advertido el error o falsedad.

El derecho a exigir la rectificación puede ser ejercido ante la falsedad, inexactitud o carácter erróneo que tenga la información que está almacenada. Su reconocimiento implica el de la preservación de la veracidad de la misma, condición que hace a la calidad.

El requisito de que los datos personales se encuentren actualizados constituye, por un lado; un derecho del titular del dato y, por el otro; una obligación que la misma ley establece para los titulares, usuarios o responsables de los bancos o archivos. La actualización significa preservar la vigencia del dato, implica que éste, sea pertinente, adecuado y cierto. La actualización es fundamental, dado que la información que los datos proporcionan puede ser utilizada para establecer categorizaciones o perfiles de los titulares, los que resultarán inexactos o erróneos, si se realizan sobre la base de informaciones que son obsoletas o desactualizadas.

En ambos supuestos –artículos 14 y 16- la LPDP ha establecido, con gran acierto, la obligatoriedad del ejercicio del derecho de acceso previo, como condición para poder entablar la acción de protección de datos personales, instancia prejudicial que algunos tribunales exigían y otros no30[30].

Para que la vía judicial sea procedente, tiene que existir una negativa, expresa o implícita, del responsable de los datos. A nuestro criterio, resulta incoherente atiborrar los tribunales de causas, simplemente para acceder o modificar un dato. Además, si se reputara inconstitucional la instancia prejudicial, se estaría obligando al titular de los datos a litigar innecesariamente.

Por lo que guarda relación directa con el principio de proporcionalidad o razonabilidad, la circunstancia de que deba realizarse la petición al archivo o registro, donde se encuentre el dato al que deseo acceder o modificar, antes de utilizar la vía judicial directamente.

La LPDP les da a los titulares de los datos un remedio rápido, idóneo y eficaz, como lo es el poder acceder en forma directa, sin necesidad de intervención judicial y el

---

30[30] En efecto, la Cámara Nacional de Apelaciones en lo Comercial, antes de la sanción de la Ley 25.326, se había pronunciado a favor de la exigibilidad de la vía prejudicial, acreditada en forma fehaciente, como requisito de procedencia para la interposición de la acción de habeas data en el fallo *"Figueroa Hnnos"* (CNCom, Sala D, del 13/5/96). Sin embargo, la Cámara Nacional de Apelaciones en lo Civil se ha pronunciado sentido contrario, descartando el cumplimiento con carácter previo de agotar la vía prejudicial en el fallo *"Bacigaluz"* (CNCiv, Sala B, del 30/12/1998) donde estableció que no constituye requisito de admisibilidad de la acción de hábeas data entablada contra una entidad privada que con carácter previo a la demanda se requiera a aquélla, la información que pudiera tener registrada respecto del requirente.

agotamiento de la vía prejudicial se convierte en un recaudo que debe ser analizado por los tribunales con carácter previo a dar curso a la demanda pertinente.

Si bien el constituyente ha querido brindar una tutela efectiva al derecho a la intimidad, lo cierto es que el legislador al reglamentar el precepto ha querido simplificar esa tutela, dándoles a los titulares de los datos la posibilidad de acceder en forma directa al registro. La circunstancia fáctica de poder acceder de forma directa a los registros de bancos de datos personales contribuye a simplificar el ejercicio del derecho, de un modo rápido y eficaz, lo que importa evitar litigios innecesarios y hace que el principio de economía procesal sea aplicado de un modo práctico[31][31].

c. El Órgano de control.

El sistema de protección de datos personales ideado por el legislador y plasmado en la LPDP presenta dos aristas, que conforman un régimen mixto de protección de dichos datos, semejante al europeo. En efecto, por un lado; la ley reconoce a los titulares los derechos de información, acceso, rectificación, actualización o supresión y, por el otro, establece un órgano administrativo de control, con atribuciones de asesoramiento, reglamentación, fiscalización y también sancionatorias.

El régimen de la Ley 25.326, se caracteriza por tender tanto a la tutela preventiva como a la reparación, a diferencia de otros regímenes como el norteamericano, que presenta un fin más bien reparador y no tuitivo, en donde los conflictos que pudieran surgir en la materia son de exclusiva responsabilidad del Poder Judicial, y no de otras entidades o autoridades intermedias, las que tienen un rol sólo complementario en este proceso reparador[32][32].

El artículo 29 pone en cabeza de la Dirección Nacional de Protección de Datos Personales –DNPDP- numerosas atribuciones, estableciendo, en el primer párrafo, el principio general en la materia. La DNPDP, tiene jurisdicción sobre todos los registros públicos y privados destinados a proporcionar información a terceros, sobre los cuales puede ejercer todas las facultades conferidas. Sin embargo, aunque no se encuentra en las Provincias, se ha ideado una red de protección que funciona en coordinación con los organismos de contralor provinciales.

Entre sus funciones, la ley asigna la asistencia y asesoramiento a las personas que lo requieran acerca de los alcances de la norma y de los medios legales pertinentes para la tutela de sus derechos, al mismo tiempo que faculta al órgano de control a dictar normas administrativas y de procedimiento.

Asimismo, el legislador le encomienda al Órgano de control, el diseño de los instrumentos adecuados para la mejor protección de los datos personales de los ciudadanos y el cumplimiento de la legislación de aplicación. Estas facultades

---

31[31] PELUFFO, María Laura, “Habeas data. Requisitos de admisibilidad de la acción de protección de datos personales.” Revista Jurídica de UCES, Nº 12, otoño de 2008, p. 144/152.

32[32] PEYRANO, Guillermo F; “Régimen legal…” . Op. Cit. p. 259/260.

normativas, agregan un escalafón más a la pirámide normativa en materia de protección de datos personales que son las normas o Resoluciones sancionadas por la DNPDP.

También, corresponde a la Dirección, una tarea de índole fiscalizadora en el ejercicio de las funciones de registración. Justamente, la norma establece que la DNPDP debe *"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".* Tarea que no se agota simplemente en el contralor del Registro, sino, que se extiende también al control del funcionamiento del mismo. De tal forma, es facultad de la Dirección, juzgar y sancionar las infracciones que se cometan en violación, tanto a la ley, como a los reglamentos que el Poder Ejecutivo dicte.

Otro punto relevante en esta tercera fase, lo constituye el artículo 21 de la LPDP, al reglamentar el Registro, una de las herramientas indispensables para dotar de eficacia a la ley, conjuntamente con el Órgano de control y las sanciones que el mismo aplica en caso de incumplimiento de la norma[33][33]. En tal sentido, la normativa regula el Registro, prescribiendo no sólo los requisitos de inscripción, sino también los supuestos especiales.

Así, siguiendo el criterio adoptado por el constituyente, la norma establece el deber de inscripción en el Registro Público de todo registro, archivo, o base de datos público y privado destinado a brindar información a terceros.

Este requisito ha sido entendido como un recaudo de licitud, del accionar de los bancos de datos[34][34], en los términos dispuestos en el artículo 3° de la LPDP en tanto dispone que *"la formación de archivos de datos será lícita cuando se encuentren debidamente inscriptos".* Esto significa que la inscripción debe concebirse como un requisito para el funcionamiento de todo archivo, registro, base o banco de datos; debiendo los mismos, en consecuencia, obtener la inscripción en el registro correspondiente con carácter previo al inicio de las diferentes operaciones de tratamiento de informaciones.

La necesidad de una inscripción de tal naturaleza, representa la primer medida y quizás la más eficaz, para viabilizar el control que la ley le asigna a la autoridad pública en la actividad de manejo de datos[35][35]. En tal sentido, otorga operatividad y eficacia también a otras disposiciones contenidas en la LPDP.

La norma exige la inscripción de los bancos de datos privados que exceden el uso exclusivamente personal o profesional, y los que tienen como finalidad la cesión o

---

33[33] BASTERRA, Marcela I., "Protección de datos personales. Ley 25.326 y Dto 1558/01. Comentados…" Op. Cit. p. 453/461.

34[34] UICICH, Rodolfo Daniel, Habeas Data. Ley 25.326, Editorial Ad Hoc, Buenos Aires, 2001, p. 101.

35[35] CARRANZA TORRES, Luis R, Habeas data: la protección jurídica de los datos personales, Ediciones Alberoni, Córdoba, 2001, p.110.

transferencia de datos personales, sin perjuicio de que la circulación de la información producida sea a título oneroso o gratuito. Todo ello, en concordancia con el artículo 24 de la ley, que exceptúa de la obligación de registración a los titulares de archivos que sean de uso exclusivamente privado, como puede ser una agenda personal, o el registro de datos de una empresa para uso interno que no será dado a conocer a terceros.

Por último, cabe destacar que el criterio para el otorgamiento de la misma a un banco de datos tanto público como privado, debe limitarse al contralor formal del cumplimiento de los requisitos exigidos en el mencionado artículo 21, y a las demás disposiciones legales aplicables, sin que pueda rechazarse por razones de oportunidad y conveniencia. Por esto, en caso de rechazo, el solicitante puede insistir por medio de la vía administrativa recursiva.

3. Conclusiones.

La acción de protección de datos personales cubre el requerimiento social estableciendo una solución; por un lado, a los aspectos relacionados con la regulación de los datos de las personas físicas y de las de existencia ideal; por el otro, a la necesidad de reglamentación de los bancos o registros de datos; ya sea privados, destinados a proveer informes y de los registros públicos.

El legislador ha logrado un equilibrio entre el derecho a la información y el derecho a la intimidad, que en definitiva son bienes jurídicos igualmente ponderables, cuya colisión, el habeas data intenta compatibilizar.

Los derechos fundamentales constituyen la base de la moderna igualdad que es precisamente una igualdad en *drotis,* en cuanto hacen visibles dos características estructurales que los diferencia de todos los demás derechos. En primer lugar, su universalidad, es decir, el hecho de que corresponden a todos y en la misma medida; al contrario de lo que sucede con los derechos patrimoniales, que son e*xcludendi alios,* de los que un sujeto puede ser o no titular, pero que cada uno lo es, con exclusión de los demás. En segundo lugar, su naturaleza de indisponibles e inalienables -tanto activa como pasiva- significa, que los sustrae del mercado de la decisión política, limitando la esfera de lo decidible, vinculado a su tutela y satisfacción[36][36].

En Argentina, hay una legislación -Constitución y leyes- que goza de excelentes estándares en materia de protección de datos personales. Lo que implica un paso adelante en la salvaguarda de un aspecto del derecho fundamental a la intimidad; derecho que es necesario apuntalar especialmente, porque a la luz de los avances tecnológicos producidos a partir del siglo XX se encuentra debilitado, toda vez que no hay remedios jurídicos suficientes que puedan establecer un equilibrio. La garantía de habeas data es sólo el punto de partida, pero a la vez, otorga la armonía

36[36] FERRAJOLI, Luigi, Derechos y garantías. La ley del más débil, Editorial Trotta, Madrid, España, 2004, p. 23.

indispensable, ante la necesidad de ponderación de estos derechos de igual jerarquía e importancia; el derecho a la información y el derecho a la intimidad.