

HABEAS DATA

Marcia MUÑOZ DE ALBA MEDRANO

SUMARIO: I. *Introducción*. II. *Concepto*. III. *Diferencias conceptuales*. IV. *Conceptos relevantes*. V. *Antecedentes*. VI. *Clasificación del habeas data*. VII. *Derechos que protege el habeas data*. VIII. *Tipos de habeas data*. IX. *La protección de datos personales, recurso no jurisdiccional. Europa: Alemania*. X. *La protección de datos personales en organismos públicos*. XI. *La protección de datos personales en Latinoamérica: recurso procesal*. XII. *Bibliografía*.

I. INTRODUCCIÓN

La raíz etimológica de ambas voces utilizadas (*habeas* y *data*) es explicada por Cretella Júnior, quien menciona “análogamente al *habeas corpus*, la expresión *habeas data* es formada del vocablo *habeas*, y *data*, acusativo neutro plural de *datum*, de la misma raíz que el verbo latino *do, das, dedi, datum, dare* igual a “dar”, “ofrecer”. *Datum*, singular de *data* es empleado por Propercio, en las *Elegías*, libro III, Elegía 15, verso 6: “*nullis capata Lycina datis*” y por Ovidio, en las *Metamorfosis*, libro VI, verso 363, ambos con el sentido de “presentes”, “donativos”, “ofertas” y no con el sentido de “datos”. Los diccionarios de la lengua inglesa traducen “*datum*”, plural “*data*”, por “*facts*”, “*things certainly known*”; “*no or available*”.

En portugués, el *data* es traducido por “documentos”, “datos” (común en el lenguaje de la informática: procesamiento de datos). “Datos” son “informaciones”, que constan en archivos, en bancos de datos. “Informaciones relativas a las personas, que constan en registros o bancos son datos.

Así *habeas data* al pie de la letra significa: “toma los datos que están en tu poder y entrégalos al interesado” o “brinda al interesado, mediante cer-

tificación, todos los datos o documentos que se encuentran en tu poder que pueda defender él sus derechos en juicio”.¹

II. CONCEPTO

Recurso procesal diseñado para controlar la información personal contenida en bancos de datos, cuyo derecho implica la corrección, la cancelación, y la posibilidad de restringir y limitar la circulación de los mismos. Adoptado este concepto por diversos países latinoamericanos, simulando el recurso del *habeas corpus* que protege la libertad, el *habeas data* protege la información nominativa, es decir, aquella que identifica al individuo.

La fórmula utilizada por el Tribunal Constitucional alemán en 1983, el “derecho a la autodeterminación informativa”, tuvo por objeto garantizar la facultad de las personas para conocer y tener acceso a las informaciones que les conciernen, las cuales son archivadas en bancos de datos para controlar su calidad, lo cual implica la posibilidad de corregir o cancelar los datos inexactos o indebidamente procesados y disponer sobre su transmisión.²

La Corte Constitucional colombiana la ha definido como el derecho autónomo fundamental que permite a toda persona conocer, actualizar y rectificar las informaciones que sobre ella hayan sido consignadas en bancos de datos y en archivos de entidades públicas o privadas. Esto en defensa de los derechos fundamentales como la intimidad, la honra y buen nombre (Sentencia T-094/95).

III. DIFERENCIAS CONCEPTUALES

Encontramos diferentes interpretaciones del término en la doctrina especializada, con la denominación “libertad informática”. Pérez Luño alude a un nuevo derecho fundamental propio de la tercera generación, el cual tiene por objeto “garantizar la facultad de las personas de conocer y tener acceso a las informaciones que les conciernen, archivadas en bancos de datos; controlar su calidad, lo que implica la posibilidad de corregir o can-

¹ Puccinelli, Óscar, *El Habeas data en Indoiberoamérica*, Bogotá, Temis, 1999, p. 296.

² Lucas Murillo de la Cueva, Pablo, *Informática y protección de datos personales*, Madrid, Centro de Estudios Constitucionales, 1993.

celar los datos inexactos o indebidamente procesados y disponer sobre su transmisión”. Frosini se refiere a ella como “una nueva forma presentada por el derecho a la libertad personal... es decir, el derecho a controlar las informaciones sobre su propia persona, es el derecho al *habeas data*”. Lucas Murillo la define como “el control que a cada uno de nosotros nos corresponde sobre la información que nos concierne personalmente, sea íntima o no, para preservar de este modo en último extremo, la propia identidad, nuestra dignidad y libertad”. Para Puccinelli “es aquella protección del principio-valor-libertad que, aplicado a la actividad informática, se traduce en el derecho de los operadores de estos sistemas de coleccionar, procesar y transmitir toda la información cuyo conocimiento, registro o difusión no esté legalmente restringido por motivos razonables, fundados en la protección de los derechos de las personas o en algún interés colectivo relevante que justifique tal limitación”.

Desde el punto de vista jurídico las diferentes acepciones de la noción *habeas data* dan lugar a ciertas clarificaciones. El concepto de “la libertad informática” no especifica sobre su naturaleza, es decir, si se trata de un derecho o de una garantía; el concepto de “derecho a la protección de datos personales” comprende de manera más amplia la suma de principios, derechos y garantías establecidos a favor de las personas que puedan verse perjudicadas por el tratamiento de los datos nominativos.

Como afirma Pérez Luño: “La protección de datos personales tendría por objeto prioritario asegurar el equilibrio de poderes sobre y la participación democrática en los procesos de la información y la comunicación a través de la disciplina de los sistemas de obtención, almacenamiento y transmisión de datos”. Opinamos como Puccinelli que el término “derecho de protección de datos personales” es una denominación genérica, que “engloba todas las otras rotulaciones y conceptos, con lo cual el derecho a la autodeterminación informativa bien podría ser una especie de él”. En esa lógica, la “autodeterminación informativa” sería entonces un aspecto del derecho a la protección de datos, y el *habeas data*, su garantía, su instrumento procesal.

IV. CONCEPTOS RELEVANTES

Información nominativa o datos personales es aquella información que permite revelar la identidad de una persona física; *tratamiento automati-*

zado se refiere al proceso de recopilación de información nominativa que es introducida a un banco de datos manejado en una computadora —las normas tienden a proteger la privacidad de la persona independientemente de que la recopilación de la información nominativa sea manual o automatizada—; *informaciones sensibles* son aquellas relativas al origen racial del individuo; a las opiniones políticas, filosóficas o religiosas; a las adscripciones sindicales y aquellas relativas a las preferencias sexuales, que sólo pueden ser recopiladas con la autorización del individuo en cuestión; dato personal.

V. ANTECEDENTES

La evolución histórica del “derecho a la intimidad” está estrechamente ligada con el desarrollo del *habeas data*. Desde 1980, con la consagración del “derecho a ser dejado en paz” (*right to be left alone*) propuesto por Warren y Brandeis en el artículo “The right to privacy”, publicado en *Harvard Law Review*, el concepto de *privacy* ha ampliado notablemente su contenido. Ahora bien, la protección de los datos personales, que es un derecho que pertenece al contexto de la era informática, ha sido regulado por diversos países en el mundo con diferente formato.

VI. CLASIFICACIÓN DEL *HABEAS DATA*

Encontramos dos diferencias básicas, aquellos países que establecieron un mecanismo no jurisdiccional, principalmente los europeos, y aquellos que establecieron un mecanismo jurisdiccional a través del *habeas data*, principalmente países latinoamericanos. Puccinelli habla de *habeas data proprio* o *tradicional*: aquel destinado al derecho a la protección de los datos personales, en la concepción del espíritu europeo y el *improprio*, utilizado para garantizar el derecho de acceso a la información pública, aplicado en algunos países de Latinoamérica.

VII. DERECHOS QUE PROTEGE EL *HABEAS DATA*

El recurso de *habeas data* o el derecho de autodeterminación informativa tiene como objetivo fundamental la protección de la privacidad en el manejo automatizado o manual de datos personales. En términos generales el sujeto podrá ejercer: a) *derecho de acceso* a la información nominativa

personal en los diversos bancos de datos; b) *derecho de información* sobre el uso, destino y duración del archivo de datos personales. En los casos del *habeas impropio* se utilizará el *habeas data* para el acceso a la información pública; c) *derecho de rectificación o actualización* de la información personal; d) *derecho de reserva*, tratándose de datos que son legítimamente recopilados pero cuyo acceso sea restringido, pudiendo ser conocido sólo por aquellos legalmente autorizados. Este derecho se relaciona con el manejo de la información sensible para cuyo manejo existen determinadas previsiones específicas.

VIII. TIPOS DE *HABEAS DATA*

Néstor P. Sagues ha propuesto una clasificación de los diversos tipos de *habeas data*: a) *habeas data informativo*: cuando se utilice para obtener la información nominativa determinada, reglamentado en las Constituciones de Argentina, Brasil, Colombia, Ecuador, Guatemala, Paraguay y Perú; b) *habeas data aditivo*, aquel que trata de actualizar o incluir datos o información dentro de los archivos, regulado en las Constituciones de Argentina, Brasil, Colombia, Ecuador y Paraguay; c) *habeas data rectificador o correctivo* cuyo objetivo es corregir informaciones falsas, inexactas o imprecisas, regulado en las Constituciones de Argentina, Brasil, Colombia, Ecuador, Guatemala y Paraguay; d) *habeas data reservador*, tiene por objeto asegurar que un dato determinado sea proporcionado a quienes se encuentran legalmente autorizados para conocerlo; e) *habeas exclutorio o cancelatorio*: se trata de eliminar información almacenada en algún banco de datos o sistema de información, tiene relevancia para aquella información considerada como sensible, regulado en las Constituciones de Argentina, Ecuador y Paraguay.

IX. LA PROTECCIÓN DE DATOS PERSONALES, RECURSO NO JURISDICCIONAL. EUROPA: ALEMANIA

A principios del siglo XX, en pleno proceso de despegue del constitucionalismo social, se gestó en Alemania la simiente de lo que posteriormente sería el derecho a la protección de los datos nominativos. El derecho a controlar la información de índole personal nace, en el plano constitucional, en 1919, fecha en la que la Constitución de Weimar otorgó a los fun-

cionarios públicos, entre otros, el derecho a examinar su expediente personal (artículo 129). Es hasta el 1o. de enero de 1970 cuando el *Land of Hesse* adopta la primera ley federal para la protección contra el abuso de datos sobre las personas con motivo del tratamiento electrónico de los mismos, documento en el que se crea la figura de un funcionario encargado de velar por el cumplimiento de la ley. Esta norma de aplicación a los registros automáticos y manuales del sector público y privado en los que se procesen datos relativos a las personas físicas, exige el consentimiento del interesado, previo el registro del dato; regula el derecho de acceso; establece obligaciones del responsable del registro respecto a la adopción de medidas de seguridad pertinentes para informar al ciudadano acerca del registro de sus datos, establece un organismo de control del contenido de la materia.

Entre otras normas de países europeos, dictadas en la década de los sesenta, tenemos: *Suecia*: con *Data Lag* de 1973 —la primera norma de alcance nacional en Europa, ya que la alemana era sólo de vigencia en el *Land*— que crea un registro público específico, obligado a registrar los archivos electrónicos de datos personales de carácter público o privado; establece la obtención de licencias para gestionar el registro de datos personales; y tratándose de datos personales sensibles se determinó la autorización expresa de la inspección de datos, que es el órgano encargado de la aplicación de la ley. *Francia*: con su *Loi relative à l'informatique, aux fichiers et aux libertés* —ley relativa a la informática, los ficheros y la libertad—, del 6 de enero de 1978, creó la Comisión Nacional de Informática y Libertades con facultades reglamentarias, de control y protección al público. En materia de recolección y tratamiento de datos, prohíbe actuar sobre datos sensibles sin consentimiento expreso de la persona a la cual pertenecen; ante la comisión se realiza el procedimiento administrativo para tener acceso o impugnar la información personal o sensible o pública. *Austria*, con su *Federal Data Act* —Ley Federal de Datos— del 18 de agosto de 1978 concede el derecho fundamental a la protección de datos, tanto a las personas físicas como a las jurídicas frente a los registros públicos y los privados. En cuanto a los datos nominativos, éstos sólo pueden obtenerse cuando se trate de bancos públicos de datos; se creó la Comisión de Protección de Datos con facultades de índole administrativa y judicial. *Dinamarca*, con la *Public and Private Authorities Registers Act* —Ley de los registros de autoridad pública y privada—, sancionada el 8 de junio de 1978, regula en dos cuerpos diferentes los registros del sector público —con excepción de los servicios de información policiales y de las fuerzas

de seguridad encargadas de la defensa nacional— y los del sector privado—con excepción de los que se lleven con fines científicos y estadísticos—. Los registros públicos deben contar con la previa autorización ministerial de funcionamiento bajo el control de la Inspección de registros y sólo pueden contener datos necesarios, para cumplir con las tareas que se les adjudican. *Noruega*, con su ley sancionada el 9 de junio de 1978, que se aplica a los registros de cualquier tipo, es decir, automatizados o manuales, públicos o privados, y deben contar tanto con la autorización previa de funcionamiento y para tratar información sensible y transferir los datos transfrontera. Del mismo modo se crea el organismo “Inspección de datos” que tutela, entre otras cosas, los datos personales. *Inglaterra* cuenta con la *Data Protection Act* del 12 de julio de 1984. *Portugal*, país que protege a nivel constitucional el derecho a la autodeterminación informativa, nos dice en su artículo 35: “Todos los ciudadanos tendrán derecho a tomar conocimiento de los datos constantes en ficheros o registros informáticos a su respecto y del fin a que se destinan, pudiendo exigir su rectificación y actualización, sin perjuicio de lo dispuesto en la ley sobre secreto de Estado y secreto de justicia”. A nivel reglamentario se expidió la ley 10/91 de la protección de datos personales frente a la informática, del 19 de febrero de 1991 y promulgada el 9 de abril de 1991. Por otra parte fue creada la Comisión Nacional de Protección de Datos Personales Informatizados, autoridad responsable y encargada de la correcta aplicación de estos ordenamientos y se establecen requisitos para el tratamiento de la información sensible. *España*, también a nivel constitucional, en su artículo 18.4 determina: “La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos”. A nivel reglamentario, con la Ley Orgánica de Regulación del Tratamiento Automatizado de Datos del 29 de octubre de 1992, y con el espíritu de salvaguardar el derecho al honor, a la intimidad personal y familiar y a la propia imagen, establece mecanismos cautelares por las violaciones a la privacidad que pudieren resultar del tratamiento de la información personal. Por otra parte, fue creada la Agencia de Protección de Datos como autoridad encargada de la aplicación de la norma. *América: Estados Unidos*, con una tradición clásica en la protección del derecho a la privacidad cuenta con la *Freedom Information Act*—Ley de libertad de información—, sancionada en 1966, en la que se consagra el principio según el cual la información contenida en los documentos públicos es de libre acceso para los ciudadanos norteamericanos;

en 1970 se aprobó la *Fair Reporting Act*, Ley de información crediticia correcta, que protege al cliente de establecimientos de crédito contra la violación de su privacidad por parte de las agencias de información; en 1974 se introdujo la *Privacy Act* —Ley sobre la privacidad— que se aplica a las informaciones sobre personas físicas, cuyos nombres se encuentren contenidos en registros del gobierno federal, estableciendo que las agencias públicas sólo podrán recabar registros de datos personales que guarden relación con los fines para los cuales han sido creadas, además de estar obligadas a obtener dicha información directamente del sujeto en cuestión, de mantenerla actualizada y conceder al individuo el derecho de acceso a la misma; se establecen restricciones de acceso a los archivos elaborados por la CIA, FBI, servicios de inmigración y registros contra la lucha de tráfico de drogas. Para la difusión de datos de registros personales se deberá contar con el consentimiento expreso del interesado.

X. LA PROTECCIÓN DE DATOS PERSONALES EN ORGANISMOS PÚBLICOS

1. *El Consejo de Europa*

En la esfera regional europea —en la americana no han dictado disposiciones similares al respecto—, son de aplicación obligatoria las disposiciones contenidas en el Convenio del Consejo de Europa de 1981, así como las de la directiva relativa a la protección de datos personales de 1995. En el plano regional europeo, el Parlamento Europeo, reconociendo la urgencia de la libertad individual y la informática, adoptó el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, aprobado en Estrasburgo por los Estados miembros del Consejo de Europa en 1981, a cuyo tenor, cada parte debía adoptar, en su derecho interno, medidas necesarias para la protección de los datos mencionados. Este documento fue fundamental en el posterior desarrollo de las normas locales, ya que se establecieron principios básicos sobre: la protección de datos; el flujo de datos transfronterizo; el tratamiento automatizado de datos personales en los sectores público y privado; las obligaciones de confidencialidad y de obtención de consentimiento para los generadores de bancos de datos; así como los derechos de los usuarios de los mismos. Posteriormente, en 1995, el Parlamento Europeo y el Consejo de Europa pactaron una directiva 95/46/CE, relativa a la pro-

tección de datos personales, en la que se precisaban los conceptos del convenio de 1981, entre los temas que se trataron, estaban: a) Principios relativos a la calidad de los datos. b) Principios relativos a la legitimación del tratamiento de datos. c) Categorías especiales de tratamientos. d) Información del interesado. e) Derecho de acceso del interesado a los datos. f) Excepciones y limitaciones. g) Derecho de oposición del interesado. h) Confidencialidad y seguridad del tratamiento. i) Notificación. j) Recursos judiciales, responsabilidad y sanciones. k) Transferencia de datos personales a países terceros. l) Códigos de conducta. m) Autoridad y control y grupo de protección de las personas en lo que respecta al tratamiento de datos personales. Posteriormente, el 14 de junio de 1985, se aprobó el Acuerdo de *Schengen* entre los gobiernos de los Estados de la Unión Económica de *Benelux*, de la República Federal de Alemania y de la República Francesa, relativo a la supresión de las fronteras comunes, en cuyo título VI se contempló “la protección de datos de carácter personal” (artículos 126 a 130). El 17 de septiembre de 1987 el Comité de Ministros del Consejo de Europa dictó la recomendación R-87, tendiente a reglamentar la utilización de datos de carácter personal en el sector policial. En el plano específico, la Unión Europea adoptó el 12 de abril de 1989 la Declaración de Derechos y Libertades Fundamentales, en la que específicamente se otorgan los derechos de acceso y rectificación respecto de los documentos administrativos y datos de las personas afectadas por ellos (artículo 18). La labor del Consejo de Europa en esta temática ha sido destacada, ya que a través de sus recomendaciones se han establecido principios básicos en el tratamiento de diversos temas como el médico, estadístico, investigación científica, *marketing* y de seguridad social.

2. La Asamblea General de la ONU

En el ámbito internacional, la Asamblea General de la ONU encomendó al secretario general de la organización, por medio de la resolución 2450 (XXIII) de 19 de diciembre de 1968, la realización de un estudio para determinar las consecuencias sobre los derechos de las personas que conlleva el uso de la electrónica y los medios por los cuales podrían ser mitigados. El 10 de noviembre de 1975, la Asamblea General, reconociendo los diversos efectos de las nuevas tecnologías, adoptó la Declaración sobre la utilización del progreso científico y tecnológico en interés de la paz y en beneficio de la humanidad. Posteriormente, en la resolución 45/95 del 14

de diciembre de 1990 se aprobaron los Principios rectores para la reglamentación de los ficheros computadorizados en datos personales. La norma es de aplicación a todos los ficheros computadorizados, tanto público como privado, manuales o automatizados, e incluso para ficheros de personas jurídicas que contengan, en parte, información de personas físicas. Esta norma se divide en dos partes: “Principios relativos a las garantías mínimas que deberían preverse en la legislación nacional” y “Aplicación de principios rectores a los ficheros de organizaciones internacionales gubernamentales”. Los principios que reconoce son: la licitud y lealtad de la recolección de datos; la exactitud de los mismos (debiendo ser actualizados periódicamente); la finalidad con la que se recopila la información personal, no contrarios a la Carta de las Naciones Unidas; el derecho de acceso de la persona interesada; la no discriminación por la divulgación de la información y la seguridad de los mismos.³

3. *La Organización Mundial del Comercio*

Por su parte la Organización para la Cooperación Económica y el Desarrollo (OCDE) abordó el estudio del tema debido a la preocupación de algunos países (en particular Estados Unidos), quienes temían que las legislaciones nacionales crearan barreras proteccionistas al comercio internacional. En 1978 se acordó formar un grupo de expertos encargado de estudiar la problemática de las transmisiones internacionales de datos personales y no personales y de desarrollar directrices al respecto. En 1980 el Consejo de Ministros de la OCDE aprobó la “Recomendación relativa a las directrices aplicables a la protección de la vida privada y a los flujos transfronterizos de datos personales”.

XI. LA PROTECCIÓN DE DATOS PERSONALES EN LATINOAMÉRICA: RECURSO PROCESAL

Los principios europeos e internacionales fueron recogidos por el derecho constitucional latinoamericano, tomando diversas particularidades: a) aquellas que reconocieron derechos concretos de los registrados, como en Colombia y Guatemala; b) aquellos que adicionaron a tales derechos la previsión expresa de que los magistrados deben intervenir para garantizar

³ Puccinelli, Óscar, *op. cit.*, nota 1, p. 143.

el cumplimiento de tales derechos, como en Paraguay; c) estableciendo un proceso constitucional específico de garantía denominado o no *habeas data*, como sucede en Argentina, Brasil, Ecuador y Perú. Analicemos los casos latinoamericanos.

1. Argentina

En el artículo 43 constitucional establece:

Toda persona podrá interponer esta acción —se refiere al amparo—, para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o privados destinados a proveer informes y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos. No podrá afectarse el secreto de las fuentes de información periodística.

Para el caso argentino, el *habeas data* es una variable o subtipo de amparo. Se trata de un amparo especializado que por su inserción normativa constituye un proceso constitucional. Según la jurisprudencia argentina, se ha determinado que este recurso tiene cinco objetivos principales: a) que una persona pueda acceder a la información que sobre ella conste en un registro o banco de datos; b) que se actualicen datos atrasados; c) que se rectifiquen los datos inexactos; d) que se asegure la confidencialidad de cierta información legalmente obtenida para evitar su conocimiento por terceros; e) que se suprima del registro la llamada “información sensible” —vida íntima, ideas políticas, religiosas o gremiales— (C. Nac. Cont. Adm. Fed., 4a. sala, 5/9/95, Farrel, Desmond A. vs. Banco Central de la República Argentina y otros). Sobre los bienes jurídicos tutelados: se trata principalmente del derecho a la intimidad —incluida la intimidad familiar— y la discriminación en sentido amplio —laboral, cultural, artística, política, sindical—. Especialistas afirman que la falta de definición constitucional al respecto puede incluso extenderse a otros bienes jurídicos como el honor, la dignidad, la autodeterminación informativa y la discriminación. “Se trata de proteger a la persona frente a la indefensión por el mal uso y la publicidad de sus datos”,⁴ a la imagen.⁵ Con relación al sujeto activo, se entiende

⁴ Bidart Campos, J. Germán, “La informática y el derecho de la intimidad”, *E. D.*

⁵ Vanossi, Jorge R., “El *habeas data* no puede ni debe contraponerse a la libertad de los medios de prensa”, *E. D.*

que este derecho es válido para persona moral o física; sobre el sujeto pasivo se trata de una norma aplicable a archivos públicos y privados, quedando excluidos aquellos de los servicios de inteligencia y los generados en el ámbito periodístico —en cuanto al acceso a datos de esta naturaleza—. El *habeas data* también ha sido integrado a algunas de las Constituciones de las provincias argentinas como Ciudad Autónoma de Buenos Aires (artículos 14 a 16); Provincia de Buenos Aires (artículo 20, inciso 3o.); Provincia de Catamarca (artículo 11), Provincia de Córdoba (artículo 50); Provincia de Corrientes (artículos 184 y 185); Provincia Chaco (artículo 19); Provincia de Chubut (artículo 56); Provincia de Formosa (artículo 10); Provincia de Jujuy (artículo 23); Provincia de La Pampa (artículo 17); Provincia de La Rioja, no lo regula puntualmente pero reconoce los problemas de las personas involucradas en el tratamiento de datos; Provincia de Río Negro (artículo 20); Provincia de Salta (artículo 22); Provincia de San Juan (artículo 26); Provincia de San Luis (artículo 21); Provincia de Santa Cruz (artículo 15); Provincia de Santiago Estero (artículo 60); Provincia de Tierra de Fuego, Antártica e Islas del Atlántico Sur (artículo 45); Provincia de Tucumán, se tiene elaborado en un proyecto de Código Procesal Constitucional en su artículo 34.

2. *Brasil*

Establece en el artículo 5o. constitucional:

Todos son iguales ante la ley, sin distinción de cualquier naturaleza. Se garantiza a los brasileños y a los extranjeros residentes en el país la inviolabilidad del derecho a la vida, a la libertad, a la igualdad, a la seguridad y a la propiedad, en los términos siguientes: XXXIII. Todos tendrán derecho a recibir de los órganos públicos informaciones de su interés particular, o de interés colectivo o general, que serán entregadas en los términos que establezca la ley, bajo pena de responsabilidad, excepto aquellas cuyo secreto fuere imprescindible para la seguridad de la sociedad y del Estado; 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 prefiera hacerlo por procedimiento secreto, judicial o administrativo; LXXVII. Son gratuitas las acciones de *habeas habeas* y *habeas data* en la medida que la ley disponga los actos necesarios para el ejercicio de la ciudadanía. 1. Serán de aplicación inmediata las nor-

mas definidoras de los derechos y garantías fundamentales. 2. Los derechos y garantías indicados en esta Constitución no excluyen otras que deriven del régimen y principios adoptados por ella o de los tratados internacionales en que la República Federativa de Brasil sea parte.

Alfonso Da Silva estima que el *habeas data* consiste en un remedio constitucional destinado a provocar la actividad jurisdiccional, teniendo por motivo la acción constitucional. Otros autores opinan que es una acción constitucional de carácter civil con un procedimiento sumario. Podemos observar que en este caso se trata de dos acciones especiales de *habeas data*: el preventivo, en el sentido que previene, acautela y evita; y el correctivo, que tiene la finalidad de rectificación de informaciones incorrectas o falsas.⁶ Efectivamente se trata de un instrumento que permite al interesado exigir el conocimiento de registros y datos relativos a su persona que se encuentren en reparticiones públicas o particulares accesibles al público, con objeto eventual de solicitar su rectificación. Con relación a su naturaleza jurídica, el *habeas data* brasileño es una acción civil especial, de rito sumario. En cuanto al sujeto activo, se entiende que afirma que el sujeto titular de la acción será cualquier persona, nacional o extranjera, residente en el país; y el sujeto pasivo serán aquellas entidades gubernamentales o de carácter público y aquellas personas morales que presten servicios para el público y detentando datos referentes a personas físicas o morales. Ahora bien, en cuanto al aspecto procesal, se afirma que al no existir una ley procesal especial le serán aplicadas las normas procedimentales comunes, además de estar eximido de costas judiciales.

3. Chile

No cuenta con una norma relativa a la protección de datos personales, ni reconoce expresamente el derecho de todo ciudadano a obtener información pública. No obstante eso Puccinelli opina que este derecho puede ser inferido de la conjugación de alguno de ellos. Por otro lado, la Constitución tampoco reconoce expresamente la institución de *habeas data*, sin embargo, el tema no ha sido ajeno a la comunidad jurídica chilena, ya que en la actualidad se advierte una intensa actividad, tanto en la doctrina como en la jurisprudencia, sobre la conveniencia de constitucionalizar o no la

⁶ Puccinelli, Óscar, *op. cit.*, nota 1, p. 302.

institución. En términos generales se conoce del proyecto elaborado por la Comisión de Constitución, Legislación y Justicia, en donde se hace referencia al derecho de protección de datos, sin hacer alusión a la voz de *habeas data* y delega su protección en la norma penal o civil. Este hecho ha sido ampliamente criticado por los expertos, quienes opinan que se debe dirigir hacia la norma constitucional. Habremos de esperar la evolución de estas opiniones y del mismo proyecto.

4. Colombia

Propio o tradicional el *habeas data* es introducido de manera expresa en este país con las reformas a la Constitución de 1991. Este derecho se consagra en el artículo 15 de este ordenamiento, diciendo:

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 reconocer, 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 datos se respetarán la libertad y demás garantías consagradas en la Constitución. La correspondencia y demás formas de comunicación privadas son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial y en los casos y con las formalidades que establezca la ley.

También hay otras disposiciones relacionadas con el acceso de documentos públicos y la inviolabilidad del secreto profesional. Según Puccinelli, se trata de un *habeas data* que consagra un derecho como cualquier otro y lo ubica entre los diversos aspectos de los derechos a la intimidad (personal y familiar) y al buen nombre. Siguiendo la línea de la Constitución española, apunta al respeto de la libertad y demás garantías constitucionales en la recolección, tratamiento y circulación de datos; en cuanto al derecho de acceso a la información pública, se limita a establecerlo con naturaleza de derecho entre los “fundamentales” y de los “económicos, sociales y culturales”, pero no consagra una garantía específica para su tutela. Finalmente trata al “derecho de rectificación” tanto para los particulares como para los partidos y movimientos políticos. Sobre la naturaleza jurídica de la institución colombiana ha sido perfilada por la Corte Suprema de Justicia, la cual ha sostenido, entre otras cosas:

El *habeas data* no es otra cosa que el derecho que tienen todas las personas 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. Con su consagración expresa, el constituyente ha querido significar su voluntad de que en el tratamiento y circulación de datos se han de respetar siempre las libertas y demás garantías consagradas en la Constitución (T-0008/93). El *habeas data* es derecho autónomo y fundamental plasmado en el artículo 15 de la Constitución, permite a toda persona conocer, actualizar y rectificar las informaciones que sobre ella hayan sido consignadas en bancos de datos y en archivos de entidades públicas o privadas, en defensa de sus derechos fundamentales a la intimidad, a la honra y al buen nombre (T-094/95). Para que exista la vulneración del derecho al *habeas data*, la información contenida en el archivo debe haber sido recogida de manera ilegal, en el consentimiento del titular del dato, ser errónea o recaer sobre aspectos íntimos de la vida del titular no susceptibles de ser conocidos públicamente (T-176/95).

Por otro lado, dentro de los fallos de la Corte Constitucional, destacan los siguientes temas: a) *acceso y obtención de copias*, haciendo alusión a los expedientes médicos en instituciones públicas; b) *la actualización* con relación a los datos manejados en instituciones bancarias; c) *la confidencialidad o reserva*, en temas de la prensa, de bancos de datos oficiales, en materia tributaria, en materia de historias clínicas e información de la salud; d) *exclusión*, con relación a materia tributaria en el manejo veraz y actualizado de la información; e) *inclusión* en registros públicos para licitar, concursar o contratar obras del Estado, f) *indemnización* en caso de causar daño por manejo inadecuado de la información personal. Ahora bien, con relación a los bienes jurídicos tutelados, la jurisprudencia colombiana ha hecho pronunciamientos sobre: la intimidad personal, familiar y la inviolabilidad de la correspondencia; la dignidad; la autodeterminación informática; la libertad informática; la identidad informática; la honra, la reputación, el buen nombre y la imagen; y la salud. Sobre el sujeto activo, se entiende que toda persona física o moral goza del derecho a utilizar la acción de *habeas data*. El sujeto pasivo son entidades públicas o privadas que manejan archivos de datos personales —automatizados o manuales—.

5. Costa Rica

La Constitución no regula expresamente el *habeas data* tradicional, aunque hace referencia al derecho de libre acceso a los departamentos admi-

nistrativos, esto con el propósito de recabar información sobre asuntos de interés público no cubiertos por el secreto de Estado. También existen referencias indirectas, en otras disposiciones constitucionales, aplicables a los aspectos de fondo del *habeas data* tradicional, como son: las disposiciones referidas a los derechos de la intimidad, la *libertas* y al secreto de las comunicaciones (artículo 24); el principio de reserva o libertad (artículo 28); los principios de igualdad y no discriminación (artículo 33) y los derechos a la reparación y pronta justicia (artículo 41). Por otro lado, en el artículo 48 de la Constitución costarricense se establece que toda persona tiene derecho al recurso de *habeas habeas* para garantizar su libertad e integridad personal, y al recurso de amparo para mantenerlo o establecer el goce de otros derechos consagrados en esa Constitución. Existe, sin embargo, un proyecto de ley propuesto a la Asamblea Legislativa en 1996, denominado “Del recurso de *habeas data*”, al título III de la Ley de jurisdicción constitucional, en donde el recurso se constituye como un instrumento procesal, es decir, como un amparo especializado para salvaguardar la libertad de las personas en la esfera informática, relacionado con la protección del derecho a la vida privada. En el mencionado proyecto se establece tanto el *habeas data* propio como el impropio, procediendo este último, incluso para la información declarada como secreto de Estado, sólo que será el magistrado instructor quien deberá determinar si efectivamente esta información merece el calificativo.⁷ En cuanto al sujeto activo, el referido proyecto establece expresamente, en el artículo 74, que están legitimados para interponer el recurso de *habeas data*: las personas físicas, los herederos del difunto, ascendientes y descendientes, colaterales hasta el cuarto grado y el cónyuge, las personas jurídicas, el defensor de los habitantes y las asociaciones representativas de habitantes por actos de discriminación. En cuanto al sujeto pasivo, en el artículo 71 del mismo proyecto se indica como potencial sujeto pasivo a los registros, archivos, listados o bancos de datos, sean manuales, electrónicos o informatizados, públicos o privados.

6. Ecuador

Consagra esta figura dentro de su Constitución, en el artículo 30, estableciendo:

⁷ *Ibidem*, p. 522.

Del *habeas data*. Toda persona tiene derecho a acceder a los documentos, bancos de datos e informes que sobre sí misma o sobre sus bienes consten en entidades públicas o privadas, así como conocer el uso que se haga de ellos y su finalidad. Igualmente, podrá solicitar ante el funcionario o juez competente la actualización, rectificación, eliminación o anulación de aquellos si fueren erróneos o afectaren ilegítimamente sus derechos. Se exceptúan los documentos reservados por razones de seguridad nacional.

Ahora bien, es en el artículo 35 en donde se establece el objeto del *habeas data*, decretando: La obtención de la información; derecho de acceso directo a la información; la actualización de la información cuando se solicita su rectificación; la obtención de certificaciones o verificaciones sobre la información rectificada, eliminada o no divulgada. De la reglamentación de esta institución, podemos afirmar que se trata de una garantía constitucional y a la vez una acción. En cuanto al sujeto activo, la norma constitucional se refiere a cualquier sujeto que tenga interés en la tutela de situaciones jurídicamente protegidas, desde el sujeto afectado, hasta el defensor del pueblo. El sujeto pasivo se constituye por aquellos bancos de datos e informes que consten en entidades públicas o privadas, por lo que se entiende, que se refiere a los documentos públicos administrativos en poder del Estado y demás entes del sector público, estableciendo como sanción, incluso la destitución inmediata de aquellos funcionarios que se nieguen a cumplir con las resoluciones emitidas por jueces o tribunales en el procedimiento de *habeas data* (artículo 43).

7. México

Aunque inmersos en el proceso democratizador que el propio Estado argumenta impulsar, y a pesar de que se conocen algunos proyectos sobre la reglamentación del acceso a la información pública y el manejo de datos personales, no existe en este país una reglamentación expresa sobre el tema. Aunque existen protecciones indirectas sobre la protección a la privacidad a nivel constitucional en el artículo 6o. considerando la violación a la correspondencia privada.

Por otro lado, en la Ley de Imprenta de 1917, cuyo artículo 1o. expresa lo que se constituye como un ataque a la vida privada pero es concebido como manifestaciones maliciosas hechas en forma verbal por un medio manuscrito, o la imprenta o cualquier otra manera que expuesta o circulan-

do en público o transmitida por correo, telégrafo, teléfono, radiotelegrafía cause demérito en su reputación o sus intereses.

En forma más vinculada con el manejo de la información automatizada, la Ley del Instituto Nacional de Estadística y Geografía (Inegi), en su artículo 32 establece la obligación general de los particulares a contribuir con el Inegi en el proceso de captar, producir, procesar y divulgar información estadística; por su parte, el artículo 37 reglamenta el derecho de rectificación de los informantes, quienes podrán exigir que sean rectificadas los datos que les conciernan, al demostrar que son inexactos, incompletos, equívocos u obsoletos;⁸ sin embargo, este derecho de rectificación entra en contradicción con lo establecido en el artículo 38 que determina que la información habrá de ser recolectada de manera que se respete el anonimato de los informantes. Estas contradicciones y la falta de aplicación real de esta norma, han imposibilitado su aplicación y desde luego no consagra los puntos fundamentales del derecho a la autodeterminación informativa clásica.⁹ Habremos de esperar la nueva normatividad sobre la materia.

8. Paraguay

Incorpora en 1992 al *habeas data* en su artículo 135 constitucional, esto dentro del capítulo de garantías constitucionales, y dicta:

Toda persona puede tener acceso a la información que sobre sí misma, o sobre sus bienes, obren en registros oficiales o privados de carácter público, así como conocer el uso que se haga de los mismos y de su finalidad. Podrá solicitar ante el magistrado competente, la actualización, la rectificación o destrucción de aquellos si fuesen erróneos o afectaren ilegítimamente sus derechos.

La Corte Suprema de Justicia lo ha identificado como un recurso o una acción, como si se tratara de sinónimos (Consideraciones CSJ, en autos María del Rosario Stanley Chamorro *s/habeas data*, resuelta el 26 de junio

⁸ Meján C., Luis Manuel, *El derecho a la intimidad y la informática*, México, Porrúa, 1994, p. 112.

⁹ Muñoz de Alba Medrano, Marcia, "Derecho a la privacidad en los sistemas de información pública", *Estudios en homenaje a don Manuel Gutiérrez de Velasco*, México, UNAM, Instituto de Investigaciones Jurídicas, 2000.

de 1996). Igualmente se ha regulado el *habeas data* impuro, es decir, aquel destinado al acceso a la información pública, esto en el artículo 28 que establece: “Las fuentes públicas de información son libres para todos. La Ley regulará las modalidades, plazos y sanciones correspondientes a las mismas, a fin de que este derecho sea efectivo”. Con relación a los bienes jurídicamente tutelados, se interpreta que se trata de un derecho de acceso a la información sobre el uso de la misma, su finalidad, actualización, destrucción y rectificación. En cuanto al sujeto activo la norma constitucional hace referencia a que “toda persona” puede ejercer dichos derechos. Respecto al sujeto pasivo se trata de los registros oficiales o privados de carácter público, además de personas física o moral, pública o privada que contengan la información del sujeto activo, o bien, que perturbe el ejercicio de los derechos reconocidos de información.

9. Perú

Consagra el *habeas data* en el artículo 200 constitucional, estableciendo que: “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., incisos 5o. y 6o. de la Constitución. El artículo 2o. reglamenta:

Toda persona tiene derecho: 5o. 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 el pedido. Se exceptúan las informaciones que afectan la intimidad personal y las que expresamente se excluyan por ley o por razones de seguridad nacional. El secreto bancario y la reserva tributaria pueden levantarse a pedido del juez, del fiscal de la nación, o de una comisión investigadora del Congreso con arreglo a ley y siempre que se refieran al caso investigado. 6o. A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar.

Se ha afirmado que el *habeas data*, por su excesiva amplitud y la consecuente fragilización del amparo y por su diseño (toda vez que así regulado permite, en un contexto autoritario, su utilización para violar la libertad de información y el derecho a la información, y también en uno conservador),

sustraer determinada información económica o patrimonial de la acción de los entes públicos hacendarios.¹⁰ Se trata de una garantía procesal, cuya función es tutelar los derechos contemplados en los incisos 5o. y 6o. del artículo 2o. constitucional. Tiene dos objetivos centrales: a) garantizar el derecho de acceso a la información pública, y b) evitar que se suministre a terceros informaciones que afecten la intimidad personal o familiar. En cuanto al sujeto activo, el mismo artículo 2o. señala: “toda persona tiene derecho”, tratándose del sujeto pasivo, se trata de cualquier autoridad o funcionario o persona que vulnere o amenace los derechos protegidos en el multicitado artículo. Desde el punto de vista procesal se ha dicho que el *habeas data* es un amparo especializado y debe tramitarse como un amparo hasta que no exista una ley orgánica de garantías constitucionales que lo regule a detalle; debe tramitarse ante el juez de primera instancia en lo civil del domicilio de la parte actora. Cuando se trata de archivos judiciales o administrativos, conocerá la demanda la sala civil de la Corte Superior de Justicia, la que encargará a un juez de primera instancia su trámite.

XII. BIBLIOGRAFÍA

- ALTMARK, Daniel y MOLINA QUIROGA, Eduardo, “Régimen jurídico de los bancos de datos”, *Informática y derecho, aportes de doctrina internacional*, Buenos Aires, Depalma, 1998.
- BIDART CAMPOS, J. Germán, “La informática y el derecho de la intimidad”, *E. D.*
- GARRIGA DOMÍNGUEZ, Ana, *La protección de los datos personales en el derecho español*, Madrid, Universidad Carlos III de Madrid-Dyckinson, 1999.
- FRAYSSINET, Jean, *Informatique, fichiers et libertés*, París, Litec, 1992.
- FROSINI, Vittorio, *Informática y derecho*, Bogotá, Temis, 1993.
- LUCAS MURILLO DE LA CUEVA, Pablo, *Informática y protección de datos personales*, Madrid, Centro de Estudios Constitucionales, 1993.
- MEJAN C., Luis Manuel, *El derecho a la intimidad y la informática*, México, Porrúa, 1994.

¹⁰ Zúñiga Urbina, citado por Puccinelli, Óscar, *op. cit.*, nota 1, p. 578.

- MUÑOZ DE ALBA MEDRANO, Marcia, “Derecho a la privacidad en los sistemas de información pública”, *Estudios en homenaje a don Manuel Gutiérrez de Velasco*, México, UNAM, Instituto de Investigaciones Jurídicas, 2000.
- *et al.*, *Internet y derecho en México*, México, McGraw-Hill, 1998.
- PEREZ LUÑO, Antonio “Los derechos humanos en la sociedad tecnológica”, Lozano, Mario *et al.*, *Libertad informática y leyes de protección de datos personales*, Madrid, CEC, 1989.
- PUCCINELLI, Óscar, *El Habeas data en Indoiberoamérica*, Bogotá, Temis, 1999.
- SAGÜES, Néstor, “Subtipos de *habeas data*”, *J. A.*, 20 de diciembre de 1995.
- SALGADO PESANTES, Hernán “La jurisdicción constitucional en el Ecuador”, varios autores, *La jurisdicción constitucional en Iberoamérica*, Madrid, Dyckinson, 1997.
- VANOSI, Jorge R., “El *habeas data* no puede ni debe contraponerse a la libertad de los medios de prensa”, *E. D.*
- VELÁSQUEZ BAUTISTA, Rafael, *Protección jurídica de datos personales automatizados*, Colex, 1993.