

EL HABEAS DATA: CONCEPTUALIZACIÓN Y ELEMENTOS QUE LO CARACTERIZAN

Por

Libardo Orlando Riascos Gómez (*)

1. Etimología del Habeas Data; 2. Conceptualización del habeas Data: 2.1. En el ámbito constitucional; 2.2. En el ámbito legislativo; 2.3. En el ámbito de algunos proyectos de leyes estatutarias y en la Ley 1266 de 2008 o Ley de "Habeas Data Financiero en Colombia"; 2.4. El habeas Data en la Doctrina nacional y extranjera; **3. Elementos que configuran el Habeas Data:** 3.1. Elementos subjetivos; 3.2. Elementos materiales; 3.3. Elementos formales.

1. ETIMOLOGIA DEL HABEAS DATA

Ab initio, los términos "*Habeas Data*" que hoy universalmente conoce el ámbito del derecho como una eficaz y expedita institución jurídica constitucional y legislativa para la defensa y protección de los datos o informaciones personales y el pleno ejercicio de los derechos y las libertades constitucionales, ha tenido una explicación etimológica generalizada y homologada en los Estados latinoamericanos y principalmente en Brasil donde nace la institución con dicho nombre.

Se ha explicado que el término "Hábeas" proviene de los términos latinos: "*Habeo*" o "*Habere*" y cuya múltiple significancia sería: tener, poseer, gozar, disfrutar, exhibir, presentar, tomar, aprehender, traer, trasladar, transportar, entre otros términos sinónimos.

En cuanto a éste término como sus variados significados, los doctrinantes del derecho están totalmente de acuerdo en sus alcances y aplicaciones a la figura jurídica regulada en sus constituciones y leyes estatales. La mayoría inciden más en el significado de la posesión de algo o de alguien, y por eso argumentan que Habeo o Habere, "*significa aquí tengas en posesión... que es una acepción del verbo...segunda persona del presente subjuntivo*" ^[1]; otros insisten en el significado exhibitorio del término: "*He aquí el documento, el dato, el registro requerido*" ^[2]; algunos otros, enfatizan en que significa: "*conserva o guarda tu*" ^[3]; y hay quienes prefieren resaltar la función de aprehensión en forma poco ortodoxa, al decir: "*que el sujeto a que los datos refieren pueda haberlos, acceder a los mismos*" ^[4], o también al dominio o propiedad al decir: "*eres dueño de tus datos*" o "*tienes tus datos*" ^[5]; o bien "*para tomar conocimiento de los datos a ella referi-*

(*) Ph.D. en Derecho (Universidades de Navarra y Lleida, España). Docente TC, Titular de Derecho Público de la Universidad de Nariño (Pasto-Colombia). Iriascos@udena.edu.co

(1) SOLANO NAVARRA, Roberto J. *Contraloría Departamental del Atlántico: Informe*. En: <http://www.contraloria.atlantico.gov.co/>. En similar sentido: CHANAME ORBE, Raúl. *Hábeas Data y el Derecho fundamental a la intimidad de la persona*. En: <http://www.sisbib.unmsm.edu.pe>.

(2) AA.VV. *El Hábeas Data en el Derecho Venezolano*. En: <http://www.conhist.org/>

(3) LAMA MORE, Héctor E. *El hábeas Data en el Perú. El Estado de cosas inconstitucional en el caso Arellano Serquen contra el CNM*. En: h.enriquelama@hotmail.com. En igual sentido: BARDELLI LARTIRIGOYEN, Juan B. *El derecho de Hábeas Data en el Código Procesal constitucional y en la jurisprudencia del tribunal Constitucional*. En: <http://www.riajej.org/>

(4) FLOREZ DAPKEVICIUS, Rubén. *Garantías de los Derechos Humanos. El Hábeas Data*. En: www.monografias.com

(5) ALMIRSON, Lisandro. *Proyecto de reforma a la Constitución de Corrientes*. Constituyente. En: <http://www.senadoctes.gov.ar/>

dos y de su finalidad”^[6], y, finalmente, hay quienes rememorando el término de hábeas utilizado por siglos en la construcción de la institución jurídica de Hábeas Corpus, manifiesta que éste significa: “que se tenga, traiga, exhiba o presente los datos”^[7].

Con relación al término: “Data” discutible y discutido al menos desde el punto de vista del uso terminológico y como adición o apellido del “Hábeas”, pues en castellano, data significa “fecha, o tiempo antiguo”; en cambio, en inglés significa toda forma, hecho o suceso que identifique información alguna de algo o alguien. En informática o computación es cualquier unidad, dígito o cifra de información que puede estar representada en sonido, video, texto o imágenes^[8]. O bien, el término “data” se refiere al “acusativo neutro plural de *datum*, de la misma raíz que el verbo latino *do, das, dedi, datum, dare* = ‘dar’, ‘ofrecer’. *Datum*, singular de *data*, es empleado por Propertio, en las *Elegías*, libro III, Elegía 15, verso 6: «*nullis capta Lycina datis*» y por Ovidio, en *Metamorfosis*, libro VI, verso 363, ambos con el sentido de ‘presentes’, ‘donativos’, y no con el sentido de ‘datos’^[9].

De lo anterior se infiere que el término inglés de “Data” o datos, o del singular “Datum” dato, es el que se le aplica por agregación a la definición del “Hábeas” latino, pues como lo demuestra Puccenilli el término data no significa datos ni su singular dato en latín, como casi todos los lectores por vez primera de los términos “Hábeas Data” deducen fonológicamente. Ahora bien, qué importancia actual tiene este desfase lexical en la institución jurídica que conocemos como “Hábeas Data” donde se une una palabra latina a otra de origen inglés, para producir una sola que nos da como resultado una institución que se ha venido generalizando en todo el mundo y se entiende como tener, poseer, gozar, disfrutar, exhibir, presentar, tomar, aprehender, traer, trasladar, transportar los datos o informaciones de la persona (natural o jurídica) o de sus bienes. Institución jurídica que algunos autores como lo ut supra citados, reducen a las acciones de “acceder, tener y exhibir los datos personales”.

La importancia va más allá de lo terminológico, pues pensamos que si los constitucionalistas brasileños, quienes se asegura estructuraron en normas jurídicas locales, luego federales y finalmente en la Constitución de 1988^[10], la institución del “Hábeas Data”, debieron fundamentar esta acción constitucional de carácter exhibitorio de la libertad de información o de los datos de la persona, en figuras del antiguo derecho romano que permitían no simplemente asimilar fonológicamente el término “Hábeas Data” a “Habeas Corpus”^[11] en el primer término y distinguir el segundo, sino a la institución

(6) SANCHEZ, Mariana. **EL Hábeas Data**. En: www.ilustrados.com

(7) BAZAN, Víctor. **Revista Semestral del Centro de Estudios constitucionales**. Universidad de Talca, Facultad de ciencias jurídicas, Santiago de Chile. En: www.librotecnia.cl

(8) Ob., ut supra cit.

(9) **da-ta** [dáyte, dáttə]. *noun* (takes a singular or plural verb): 1. **factual information**: information, often in the form of facts or figures obtained from experiments or surveys, used as a basis for making calculations or drawing conclusions. 2. **information for computer processing**: information, e.g. numbers, text, images, and sounds, in a form that is suitable for storage in or processing by a computer. Plural of *datum*. En: **Enciclopedia Microsoft Corporation**. 2007.

(10) PUCCINELLI, Oscar. **El “Hábeas Data” en Brasil**. En: <http://www.astrea.com.ar/>

(11) El Hábeas Data es una institución jurídica que se deriva, es análoga, se infiere o resulta de la comparación con el Hábeas Corpus de construcción jurídica ancestral. Incluso se dice que el Hábeas data “es el hijo natural del Hábeas Corpus” en términos de Sorín. Vid. CARRANZA TORRES, Luis. **El sistema de protección de datos en Córdoba**. En: <http://www.informatica-juridica.com>. En igual sentido: el constitucionalista BIDART CAMPOS, citado por MARTELLA, Lilián, **Hábeas Data: Garantía de una Dimensión fundamental de la libertad**. En: <http://www.ceride.gov.ar/>. AA.VV. **El Hábeas Data Venezolano**. En: <http://www.conhist.org/>; SORIN, Sergio. **El Hábeas Data en Argentina: Invasión de la privacidad**. Buenos Aires, Marzo 21 de 2000.

jurídica románica que cabría asignársele en los casos de exhibición o aprehensión de datos personales. En efecto, en el derecho romano existían muchos interdictos para toda clase de acciones, actuaciones o hechos humanos. El más genérico era la "*Interdicta exhibitoria*", por la cual "*se ordena una exhibición*" de algo o de alguien, como sucedía "en el *interdictum de homine libero exhibiendo*", es decir, el "*interdicto exhibitorio y popular, por el cual se ordena al exhibición de un hombre libre que se tiene con dolo malo; se propone defender la libertad*" ^[12].

Siguiendo estos parámetros del derecho romano, para defender modernamente la libertad de informaciones o los datos, bien pudo instituirse en nuestro criterio, la "*Interdicta exhibitoria*" de acta o bien la "*Interdicta exhibitoria*" de documento; pues el término "acta" significaba, "anotar en archivo o protocolo público"; o bien "documento público" que era "el escrito redactado por un funcionario público y con valor probatorio superior al redactado por los particulares". En consecuencia, si hoy nos quedamos con el primer término y la conceptualización dada al "*Hábeas*", el segundo término sería acta o documento, por el contenido y ancestro romano. Tendríamos entonces el "*Hábeas acta*" o el "*Habeas documento*".

Sin embargo y como lo aclara *Puccenelli* ^[13] en portugués, "el *data* es traducido por 'documentos', 'datos' (común en el lenguaje de la informática: procesamiento de datos)", con lo cual creemos que la potísima razón de los Constitucionalista Brasileños y entre ellos Alfonso Da Silva a quien se estima acuñó el término "*Habeas Data*" ^[14] se debió más a la traducción del término inglés "data", por dato o documento al portugués, que a seguir los lineamientos del ancestro y figura jurídica romana del interdicto exhibitorio de acta o de documento, como era apenas lógico y jurídico.

El constitucionalismo brasileño en 1988, creó el "remedio" o acción procedimental del Hábeas Data como un mecanismo jurídico-constitucional preventivo para el acceso y el

(12) "Expresa Ada Pellegrini Grinover "que la creatividad del constituyente brasileño forjó un nuevo instrumento de tutela de la libertad de la persona, adecuado a su salvaguarda con relación a la información". Precisamente el Habeas Data fue creado por los constitucionalistas brasileños. Su antecedente más lejano se remonta al año de 1981, cuando el Congreso Académico de Pontes de Miranda, organizado por la Orden de Abogados y el Instituto de Río Grande del Sur, elaboró una "Propuesta de Constitución Democrática para Brasil", en cuyo artículo 2° se consagraba un instrumento procesal con las características del Habeas Data. Con posterioridad, la Ley N° 824, del 28 de diciembre de 1984 del Estado de Río de Janeiro, sirviéndose de "La Propuesta" elaborada por la Orden de Abogados y el Instituto de Río Grande del Sur, aprobó dicho instrumento procesal. En esa ley se establecía que las instituciones conservadas por un órgano público, estaban sujetas a la protección del mandato de seguridad, y en el caso de las entidades privadas, la tutela corría a cargo de la acción exhibidora regulada por el artículo 844.1 del código Procesal Civil. Cuando en 1986 el poder Ejecutivo convocó a una comisión de juristas, el nuevo instrumento fue elevado a rango constitucional en el Anteproyecto de Constitución que dicha comisión elaboró y en cual aparecía denominado por primera vez bajo el nombre de Habeas Data". ALCANTARA GARCIA, Erika R., et all **Procesos Constitucionales**. Estudiantes de IV año de Derecho. Universidad Privada Señor de Sipán. Chiclayo, Perú. En: erikinlokita@hotmail.com.

(13) GUTIERREZ-ALVIZ Y ARMARIO, Faustino. **Diccionario de Derecho Romano**. Ed. Reus, S.A., Madrid, 1982, p. 304

(14) PUCCINELLI, Oscar. **El "Hábeas Data"...** Ob., ut supra cit.
Conocimiento de los datos o informaciones personales y como un instrumento sancionatorio, de corrección, actualización y supresión de datos cuanto estos son incorrectos. En el desarrollo legislativo nueve años después, el Hábeas Data se convirtió en una acción exhibitoria de los datos personales de carácter civil y administrativo, según la naturaleza jurídica de las personas naturales o jurídicas que manejen los datos. El legislador volvió sus ojos al origen de la institución jurídica románica: un interdicto exhibitorio de acta o de documento.

2. LA CONCEPTUALIZACION DEL HABEAS DATA

La Institución jurídica del Hábeas Data siendo una estructuración de la doctrina constitucional latinoamericana ^[15], que ha tenido importantes desarrollos y evoluciones en la jurisprudencia de los Tribunales y las Altas Cortes (Constitucional y/o Suprema de Justicia, sala Constitucional, según el Estado Latinoamericano, como precisaremos más adelante) y que se ha concretado en proyectos de leyes y en leyes integrales, generales y sectoriales de protección de datos personales, de acceso a la información pública, de transparencia en la gestión pública, de protección a la vida privada o de protección a los datos financieros, según el Estado latinoamericano que las adopte.

Por ello, en el presente ensayo jurídico, preferimos hacer un relato conceptual de la Institución jurídico constitucional del Hábeas Data, más que una definición cerrada de la misma, pues la conceptualización nos permite, entre otros propósitos, suministrar varios elementos definidores de la Institución, realizar una labor comparativa normativa, jurisprudencial, legislativa y doctrinal del Hábeas Data, develar la naturaleza jurídica y hasta las características del Hábeas Data y por supuesto, verter en el discurso jurídico, las diferentes posturas de los tratadistas del derecho y la nuestra sobre la egregia institución.

En el ámbito de las Constituciones Estatales de América Latina, tomaremos algunas de Centro y Sur América y en el ambiente Europeo la Constitución de España. Estos textos constitucionales que obedecen a diferentes formas de Gobierno y de Estado, guardan algunas similitudes cuando han elevado a rango normativo superior, la Institución del Hábeas Data ^[16].

De igual forma analizaremos brevemente la conceptualización de la institución jurídica en el ámbito legislativo, con la expedición de leyes orgánicas de protección de datos, leyes especiales de protección del dato financiero, en leyes ordinarias de acceso a la información pública y la transparencia gubernamental, o en incluso en proyectos de leyes estatutarias, todas estas normas jurídicas con un común denominador el derecho, garantía, recurso o proceso de Hábeas Data, según el Estado que la regule.

En ámbito jurisprudencial, por la dispendiosa labor que implicaría analizar el trabajo jurisprudencial de los Tribunales Constitucionales en los Estados donde los hay, o las Salas Constitucionales, Civiles o Administrativas de la Corte Suprema de Justicia donde aquellas funcionen (v.gr. En la Argentina), sólo nos remitiremos a la jurisprudencia de la Corte Constitucional Colombia en lo que nos consta sobre el Hábeas Data.

Finalizaremos con las conceptualizaciones doctrinales de los tratadistas del derecho latinoamericano sobre el Hábeas Data y la Acción de protección de los datos del derecho ibérico.

(15) PUCINELLI, Oscar. *El Hábeas Data en el Brasil*. En: www.astrea.com

(16) Vid en: http://www.informatica-juridica.com/trabajos/La_vision_constitucional_del_habeas_data.asp y, http://www.informatica-juridica.com/trabajos/La_vision_legal_del_habeas_data_en_latinoamerica_y_europa.asp.

2.1. En el ámbito constitucional

Pese a que los textos constitucionales, por regla general no suministran definiciones o conceptos cerrados sobre las diferentes instituciones jurídicas que éstos se regulan, sobre la institución del Hábeas Data, no solo encontramos conceptualizaciones de aquella, sino además aspectos que demarcan la naturaleza jurídica, el campo de aplicación, el objeto y la finalidad de la misma e incluso los efectos jurídicos materiales y sustanciales.

Este proceder del constituyente derivado (Los Órganos legislativos competentes) o del Constituyente primario (Asambleas Nacionales Constituyentes por delegación directa de los pueblos soberanos), obedece principalmente a que cuando se regula la Institución de Hábeas Data, lleva preconcebida la idea de que al ser ésta una figura jurídica relativamente nueva, producto de las nuevas tecnologías de la información y la Comunicación (medios TIC); de la modulación con medidas de seguridad técnica, jurídica y estatal de la alta porosidad de los medios informáticos, telemáticos o electrónicos en todas las actividades de la sociedad actual y del Estado (la “cibersociedad” en el Estado virtual) y de la prevención efectiva contra los abusos o desafueros de la informática (“el poder informático”) ^[17], la regulación constitucional debe ser clara e inequívocamente conceptualizada hasta tal punto que en algunas constituciones, no siendo del resorte y técnica constitucional, se establecen excepciones, restricciones, limitaciones e incluso prohibiciones *numerus clausus*, para excluir la aplicabilidad de la institución a datos o informaciones sensibles o ultrasensibles para el Estado o para las mismas personas.

2.1.1. El Hábeas Data en la Constitución Argentina, es una acción de amparo específica de carácter jurisdiccional

El Hábeas Data en la Constitución Argentina, es una acción de amparo específica de carácter jurisdiccional contra todo acto u omisión de las autoridades del Estado o los particulares que sometan a tratamiento los datos personales contrariando el derecho o negando el acceso y conocimiento de aquellos.

La Constitución Argentina de 1994, en el artículo 43 incisos 1º instituye la acción de amparo como garantía constitucional para la defensa y protección del pleno de derechos y libertades constitucionales de toda persona contra los actos, hechos y omisiones de las autoridades estatales o los particulares, así:

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

En el Inciso 3º, la norma instituye la acción de amparo para que toda persona pueda acceder y conocer la información o datos personales que a ella le conciernen y estén recabados en bancos de datos públicos o privados, o bien para solicitar su supresión,

(17) RIASCOS GOMEZ, Libardo O. *El derecho a la intimidad, la visión ius-informática y los delitos relativos a los datos personales*. Tesis Doctoral, Universidad de Lleida (España), Lleida, 1999, p. 10 y ss. En: <http://www.tdx.cat/bitstream/handle/10803/8137/Tlorg2de2.pdf;jsessionid=16F1E64480AB7F2A906A49693D278BDF.tdx2?sequence=2>

rectificación, confidencialidad o actualización de los datos en caso de comprobar falsedad o eventualidades de discriminación en éstos. De la siguiente forma:

“Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o 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”.

Según el artículo 43 de la Constitución de la República Argentina se deduce, pues la norma no instituye el término “Hábeas Data”, que ésta es una acción de amparo específico que se adelanta mediante proceso jurisdiccional expedito y sumario ante cualquier Juez de la Nación, por parte de toda persona con el propósito de “*tomar conocimiento de los datos a ella referidos y de su finalidad*”, siempre que consten en registros o bancos de datos públicos, o privados y consiguientemente éstos estén destinados a proveer informes.

Esta acción constitucional, también se podrá impetrar en los casos de “falsedad o discriminación”, y en ésta eventualidad el Hábeas Data será para exigir la supresión, rectificación, confidencialidad o actualización de los datos informaciones que le conciernan.

Finalmente, y tras de llevar implícita la conceptualización de la institución de Hábeas Data en la norma constitucional, el constituyente argentino, prohíbe la afectación del derecho al secreto o el sigilo profesional de las fuentes de información periodística.

Sagües ^[18], considera que el instituto regulado en el inciso 3º del artículo 43 de la Constitución Argentina es aquél que el derecho comparado se llama “Habeas Data”, aunque el autor prefiere llamarla “*amparo informativo o amparo informático*”, entre otras razones, porque: (i) “origen se explica en virtud del desarrollo del llamado ‘poder informático’; (ii) El diferente tratamiento jurídico constitucional de mayor protección a “quienes hacen informática: productor, gestor y el distribuidor de datos”, y de menor defensa de sus derechos, entre ellos la intimidad de las personas, para los “registrados en los archivos o bancos de datos, ya que estos pueden contener información equivocada, antigua, falsa o con potenciales fines discriminatorios”; y (iii) El amparo informático “pretende ser una respuesta transaccional a los derechos constitucionales de registrantes y registrados, y atiende a cuestiones de fondo (los derechos de cada uno de aquellos), y de forma (el tipo de procedimiento para asegurar tales derechos).

“Amparo informático” o más universalmente “acción de Hábeas Data”, la Constitución Argentina conceptualiza a éste o aquella como una acción constitucional de amparo específico que genera un procedimiento jurisdiccional breve y sumario dirigido a garantizar, proteger y defender los datos o informaciones que les conciernen a las personas cuando se atentan contra aquellos con actos, hechos u omisiones por parte de entidades, organismos o dependencias del Estado y por actos o hechos de los particulares. Así mismo la servirá para proteger y defender los derechos y garantías previstas en la Constitución, las leyes o los tratados internacionales.

De lo anterior podemos colegir, lo siguiente: a) El Hábeas Data Argentino es de naturaleza jurídica jurisdiccional civil o administrativo, según el organismo o dependencia

(18) SAGUES, Néstor Pedro. *El Hábeas Data en Argentina (Orden Nacional)*. Revista Ius et Práxis, Facultad de ciencias jurídicas y sociales, Universidad de Talca (Chile), Chile, 1997. p.137 a 150

ante la cual se reclame el derecho o garantía constitucional;

b) El Hábeas Data es una acción procedimental de ámbito constitucional ejercitable por “*toda persona*”, lo cual incluye no sólo a las personas naturales o físicas, sino también a las personas jurídicas, morales o como las denomina el derecho argentino, personas con “existencia ideal” [19]. La protección de datos a las personas físicas, según Livellara [20], “tiene una estrecha vinculación con la esfera privada del individuo que incide en el ‘derecho a la intimidad’, como también, en nuestro criterio, a otros derechos y libertades fundamentales previstos en la Constitución por ser una garantía constitucional, por sobre todo para “*contener los abusos que puedan derivarse de la manipulación de información...el uso abusivo en el manejo de los datos... y la existencia de bancos de datos de acceso inmediato, cuyo control o acceso proporciona una considerable fuente de poder*” [21].

Palazzi [22], plantea la discusión doctrinal de si el Hábeas data solo protege el derecho a la intimidad o de la “privacidad”, como sostienen Bidart Campos, Almark y Molina y la Corte Suprema respectivamente, o va más allá a garantizar, los “valores constitucionales de verdad o igualdad”, como afirma Sagües; o “el derecho a la Intimidad o el honor con especial amplitud”, según Puccinelli. De lo anterior concluye que “*el Hábeas Data protege un ‘complejo de derechos constitucionales’ que incluyen la privacidad y la identidad, relacionados a su vez con la imagen y con los conceptos de verdad e igualdad*”.

c) El Hábeas Data genera para el impetrante un procedimiento expedito y sumario que garantiza la eficacia, celeridad y prontitud de la garantía constitucional.

d) El Hábeas Data se viabiliza para proteger y garantizar los datos de la persona en dos momentos del tratamiento o procesamiento de datos personales, siempre que se encuentre recabados en bases, bancos o registros de datos públicos o privados: (i) Para aprehender o “tomar” el conocimiento de los datos o informaciones que le conciernen; y (ii) Para solicitar la corrección, confidencialidad, actualización o supresión de la información o datos falsa o discriminatoria. Aquí el Hábeas Data además de un derecho constitucional es una garantía de igual rango.

e) La Institución del Hábeas Data no podrá afectar el derecho al sigilo o secreto periodístico. Esto porque era un aspecto celoso y reiteradamente solicitado por el gremio periodístico cuando se tocó el tema del Hábeas Data en 1994. Al incluir en la Constitución el inciso *in fine* del artículo 43 la no afectación del derecho al secreto se garantiza y protege en alto grado las fuentes periodísticas y fue del caso “*autoriza a los periodistas a recurrir a tribunales para exigir acceso a la información oficial, en juicios de carácter público*” [23].

(19) En este mismo sentido: ARMAGNAGUE, Juan F. **Constitución de la Nación Argentina comentada**. Ed. Ediciones Jurídicas Cuyo Mendoza, 1999, p. 217. Citado por LIVELLARA, Silvana. **Hábeas Data e informática crediticia. La Eventual responsabilidad civil de las entidades financieras y del Banco Central de la República Argentina por cesión y publicidad de datos inexactos**. La nominación expresa de personas de “existencia ideal” aparece en el artículo 1º de la Ley de Protección de Datos de Argentina o LPDA de 2000.

(20) LIVELLARA, Silvana. **Hábeas Data e informática...** Ob., ut supra cit.

(21) DROMI, Roberto et al. **La Constitución reformada**. Ed. Ciudad Argentina. Bs.As., 1994 p. 167. Citado por Livellara en la Ob., ut supra cit.

(22) PALAZZI, Pablo. **El Hábeas Data en el Derecho Argentino**. Revista de Derecho Informático Alfa-Redi, ISSN 1681-5726, No. 004, Noviembre de 1988.

(23) SOUMINEN, Kati. **Acceso a la información en América Latina y del Caribe**. Universidad de California, San Diego. En: <http://www.thedialogue.org/publications>

hasta antes de ser desarrollada en la ley seis años después, “con fallos —en especial los resueltos por la Corte Suprema de Justicia de la Nación— que le han otorgado una especial amplitud al instituto y lo han llevado a exceder considerablemente los contornos establecidos en el artículo 43, constitucional. Incluso, ha sido de permanente debate en el Congreso Nacional”, según lo sostiene Puccinelli^[24].

2.1.2. En la Constitución Boliviana, el Hábeas data es una acción jurisdiccional de amparo específico

En la Constitución Boliviana, el Hábeas data es una acción jurisdiccional de amparo específico instituido para proteger el acceso, conocimiento, objeción, eliminación o rectificación de los datos personales y los derechos fundamentales.

La Constitución Boliviana reformada en el 2002, en el artículo 23 intitulado “Acción de Hábeas Data” instituye expresamente la institución jurídica del Hábeas Data como un recurso jurisdiccional, según se manifiesta en el numeral 1º. Recurso o acción que podrá ser impetrado por toda persona natural o jurídica ante una autoridad judicial competente para solicitar la protección y la defensa de los datos personales y algunos derechos fundamentales en concreto. Esta acción o recurso se regula en cinco numerales, a saber:

I. Toda persona que creyere estar indebida o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético, informático en archivos o bancos de datos públicos o privados que afecten su derecho fundamental a la intimidad y privacidad personal y familiar, a su imagen, honra y reputación reconocidos en esta Constitución, podrá interponer el recurso de Habeas Data ante la Corte Superior del Distrito o ante cualquier Juez de Partido a elección suya.

II. Si el tribunal o juez competente declara procedente el recurso, ordenará la revelación, eliminación o rectificación de los datos personales cuyo registro fue impugnado.

III. La decisión que se pronuncie se elevará en revisión, de oficio ante el Tribunal Constitucional, en el plazo de veinticuatro horas, sin que por ello se suspenda la ejecución del fallo.

IV. El recurso de Habeas Data no procederá para levantar el secreto en materia de prensa.

V. El recurso de Habeas Data se tramitará conforme al procedimiento establecido para el Recurso de Amparo Constitucional previsto en el Artículo 19º de esta Constitución.

La Constitución Boliviana no solo conceptualiza el Hábeas Data al encasillarlo como una acción o recurso jurisdiccional apto para la protección de datos personales, como de los derechos constitucionales de la intimidad, la imagen, la honra y la reputación de las personas, sino que establece la legitimación para incoarla, la autoridad jurisdiccional competente, los recursos contra la decisión que se pronuncie en los procedimientos de amparo específico de Hábeas data, así como el objetivo y finalidad específica de la institución jurídico-constitucional.

(24) PUCCINELLI, Oscar. *Tipos y subtipos de Hábeas Data en América Latina*. Ed. Astrea, Buenos Aires (Argentina). En: www.astrea.com

En efecto, estima el constituyente boliviano de 2002, pues hasta antes de esa época la institución del Hábeas era poco conocida en Bolivia ^[25], que el recurso o acción de amparo específico, interpuesto por toda persona natural o jurídica tiene como objetivos y finalidades las siguientes: (i) Acceder y aprehender el conocimiento de los datos o informaciones a él concernidas; (ii) “objetar”, solicitar la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético, informático en archivos o bancos de datos públicos o privados “que afecten” su derecho fundamental a la intimidad y privacidad personal y familiar, a su imagen, honra y reputación reconocidos en esta Constitución.

Estos objetivos y finalidades del Hábeas Data permiten conceptualizarla como un instituto jurídico constitucional apto no sólo para aprehender el conocimiento de cualquier dato o información personal recabada en bancos de datos de titularidad pública como de titularidad privada, sean informatizados o no, sino cuando se hiciere necesario “objetar”, eliminar o rectificar aquellos. Si bien existe una evidente falta de buena redacción técnico-jurídica de las facultades o derechos componentes del Hábeas Data que siempre se hace recaer en las actividades de rectificación, actualización y eliminación de datos personales, la Constitución Boliviana resalta la primera y tercer facultad e introduce una nueva la de “objección” que podrá interpretarse como el derecho a refutar, impugnar o contradecir algo de alguien, y ese algo será la información o datos; de quién, se entiende de la persona física o jurídica. Obviamente que el término acción o recurso jurisdiccional lleva implícito la facultad de impugnar u objetar algo de alguien, y por tanto no parece afortunada la inclusión del verbo objetar. Más claro hubiese sido incluir la facultad que tiene toda persona de solicitar ante la autoridad competente, la actualización de los datos (“*Up date of data*” de los anglosajones) cuando han sido recabados o tratados en un banco de datos en forma no veraz, clara, incompleta, errada o vulnerando el ordenamiento jurídico vigente.

Pese a lo anterior, se puede decir que el Hábeas Data boliviano ha sido conceptualizado en forma amplia, a tal punto que el artículo 23 tiene unas características más de norma legislativa que de norma constitucional, pues establece la forma del procedimiento, los recursos contra la decisión que se adopte en aquél, como la descripción y categoría de los jueces que deben conocer de la acción o recurso de amparo específico.

Al igual que en la Constitución Argentina, el constituyente boliviano establece una prohibición constitucional para garantizar al máximo el derecho de secreto o sigilo profesional periodístico, cuando en el numeral IV, establece que el Hábeas Data “no procederá para levantar el secreto en materia de prensa”. Esto tiene unas amplias y claras explicaciones sociales, políticas, culturales y estatales vividas por el periodismo en Bolivia, tal como lo expone *Camacho Azurduy* ^[26] y que por ahora nos abstenemos de comentar.

2.1.3. El Hábeas Data en la Constitución Brasileña es una acción constitucional judicial o administrativa

El Hábeas Data en la Constitución Brasileña es una acción constitucional judicial o

(25) H., Benjamín Miguel. ***Acción de amparo relacionada con la protección de datos personales en el orden jurídico boliviano***. Revista *Ius et Praxis*, Año 3, Número 1º, Facultad de Ciencias jurídicas y sociales, Universidad de Talca, Talca (Chile), p. 161 a 164

(26) CAMACHO AZURDUY, Carlos A. ***El proceso de discusión del derecho de acceso a la información en Bolivia***. Vía Internet.

administrativa, interpuesta por toda persona para garantizar el acceso y conocimiento de los datos personales o para solicitar su rectificación y de aplicación directa e inmediata.

En el artículo 5º de la Constitución Brasileña de 1988, la Institución del Hábeas Data se regula expresamente con dicho nombre, pues no en vano ésta se estructuró en el ámbito de la doctrina constitucional brasileña y luego de regularse legislativamente a nivel local, federal llegó a la Constitución de la siguiente forma:

LXXII. Se concederá hábeas 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.

LXXVII: Son gratuitas las acciones de hábeas corpus y hábeas data en la medida que la ley disponga los actos necesarios para el ejercicio de la ciudadanía. 1. Serán de aplicación inmediata las normas 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

El Hábeas Data brasileño se conceptualiza como un “remedio” o garantía constitucional apta para la defensa y protección las informaciones o datos de las personas naturales o jurídicas concernidas, siempre que se hayan recabado en un registro o banco de datos, inicialmente de titularidad pública. Así mismo, y una vez haya aprehendido el conocimiento de dichos datos o informaciones personales y encontrándolos se entiende erróneos, incompletos, inexactos, no veraces, “antiguos” o contrarios al derecho, podrá escoger entre un procedimiento “secreto, judicial o administrativo” para solicitar la rectificación de los mismos.

Se entiende entonces que el Hábeas Data brasileño originalmente estimó que la persona concernida y afectada con los datos personales recabados en bancos de datos públicos, podría escoger entre un proceso secreto, judicial o administrativo para solicitar no el acceso y conocimiento de la información o datos, sino para impetrar la rectificación de los mismos, una vez los ha conocido por cualquier otro medio o mecanismos viables en el derecho civil o comercial, sí se trata de personas privadas; o en instrumentos jurídicos viables en el derecho público y principalmente administrativo, tales como el derecho de petición o recursos administrativos ejercitados ante autoridades gubernamentales o de “carácter público”. Siendo así la institución brasileña el Hábeas Data no es exclusivamente de carácter jurisdiccional, tal como se ha planteado en la Constitución argentina y boliviana, pues el concernido con unos datos contrarios al ordenamiento jurídico vigente tiene la opción entre instrumentos o mecanismos sustantivos (derecho de petición, reclamación o formulación de consultas) o mecanismos procesales (recursos administrativos, de reconsideración, de reclamación, según proceda) y ambos de índole administrativo, cuando la decisión es “gubernamental” o de “carácter público”; o bien el instrumento jurídico idóneo constitucional de naturaleza jurisdiccional denominado “acción de Hábeas Data”, pero en uno y otro caso con la finalidad específica de solicitar la rectificación de los datos del concernido o afectado con los datos recabados en un banco de datos público.

La institución del Hábeas Data tiene algunas connotaciones especiales: (i) Es una acción o remedio constitucional que puede ser impetrada por toda persona natural o jurídica; (ii) la acción puede incoar en procedimiento secreto, judicial o administrativo; (iii) En la vía jurisdiccional ante unos jueces y tribunales judiciales del ámbito civil y administrativo; (iv) La acción se incoa para aprehender el conocimiento y acceso de los datos o

informaciones personales del concernido; (v) Cualquiera sea la vía del Hábeas data será de carácter gratuito para que pueda ser ejercitada por toda la “población” (la traducción del texto original dice “ciudadanía”, limitando su ejercicio a los mayores de edad); y, (vi) el instituto de Hábeas Data es un derecho y garantía fundamental de aplicación inmediata. Por esa última connotación y a la vez característica del Hábeas Data brasileño, es por lo que Puccinelli ^[27], estima que el legislador del Brasil tardó en expedir una ley que desarrollara el artículo 5º, inciso LXXII de la Constitución sobre el Hábeas Data y concretarla en la Ley 9507 de 1997. Las personas concernidas y afectadas por las informaciones o datos recabadas en bancos de datos, en el lapso de nueve (9) años, acudió ante las autoridades competentes en forma directa a solicitar la aplicación del Hábeas Data constitucional por ser éste un derecho fundamental de aplicación inmediata.

2.1.4. El Hábeas Data en la Constitución Colombia es una acción de tutela específica de tipo jurisdiccional o una vía administrativa

El Hábeas Data en la Constitución Colombia es una acción de tutela específica de tipo jurisdiccional o vía administrativa que protege todas las fases del tratamiento de los datos personales y los derechos constitucionales, entre ellos el de la intimidad y el buen nombre.

La Institución jurídica colombiana del Hábeas Data se estructura a partir del inciso 1º y 2º del artículo 15, el artículo 20 y 74 de la Constitución de 1991. A saber:

“Todas las personas tiene derecho a su intimidad personal y familiar y a su buen nombre... 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”.

Agrega el inciso segundo, *“En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución”.*

El artículo 20, a su turno reza: *“Se garantiza a toda persona la libertad... (de) informar y recibir información veraz e imparcial...”*

Por su parte el artículo 74, sostiene: *“Todas las personas tienen derecho a acceder a los documentos públicos...”*

En la primera norma se encuentra el núcleo esencial del Hábeas Data, pues mientras en el inciso 1º se confiere el ejercicio de la acción de tutela específica a toda persona natural o jurídica para que pueda aprehender el conocimiento de las informaciones o datos personales que le conciernen, y una vez conocido el contenido de éstas, si lo encuentra incompleto, no veraz, erróneo, “antiguo” o contrario al derecho, podrá solicitar su actualización y rectificación, siempre que la información haya sido recabada en bancos de datos y *“en archivos de entidades públicas y privadas”* en forma manual, mecánica, escrita o electrónica (informática) ^[28]. Conocimiento, acceso, actualización y rectificación de los datos personales del concernido que afecten al manejo, uso y control de la información de la persona, como a derechos fundamentales, principalmente el derecho a

(27) PUCCINELLI, Oscar. *El Hábeas Data en el Brasil*. En: <http://www.astrea.com.ar>

(28) Hacemos una amplia explicación de los medios mecánicos y electrónicos, telemáticos o informáticos, utilizados en el tratamiento de datos personales, en la elaboración del Documento Electrónico --“E-document”-- y en la tipificación de las nuevas conductas delictivas sobrevenidas por la abusiva o ilegal utilización de las nuevas tecnologías de la información y la comunicación (medios TIC) y la informática. RIASCOS GOMEZ, Libardo O. *La Constitución de 1991 y la Informática Jurídica*. Ed. UNED, Universidad de Nariño, Pasto, 1997, p. 10 y ss.

La intimidad personal y familiar y a su buen nombre.

La primera parte del inciso 1º del artículo 15 constitucional, establece en nuestro criterio una especie de *Hábeas Data administrativo*, si el concernido con los datos ejercita el derecho de petición (artículo 23, constitucional) y/o los recursos administrativos ordinarios o extraordinario previstos en el Código de Procedimiento Administrativo y Contencioso-administrativo o C.P.A y C.A (artículos 74 y ss., y 93 y ss.) para solicitar la aprehensión o acceso de los datos personales y lo hace ante una persona de derecho público de cualquier nivel administrativo (Nacional, Distrital, Departamental, Municipal y corregimental), ante una persona de derecho privado con función o servicio público (artículo 2º C.P.A. y C.A.). Esto sin perjuicio de ejercer la “acción de tutela” ante los jueces individuales y autoridades, tribunales y Altas Cortes judiciales que forman parte de la jurisdicción constitucional colombiana y según los factores de competencia, ejercicio de la acción utilizado como mecanismo transitorio para defender o garantizar el derecho fundamental de petición, o bien ejercida directamente cuando se ha agotado previamente los mecanismos administrativos o jurisdiccionales pertinentes y no existe otro remedio jurisdiccional o administrativo para tutelar un derecho fundamental (artículo 86 constitucional y Decreto 2591 de 1991). Si se ejercita la acción de tutela en una de las dos formas para aprehender el conocimiento y/o acceso a la información o datos personales del concernido, decimos que emplea el *Hábeas Data jurisdiccional* en esta fase del tratamiento de datos.

Iguales reglas previas o concomitantes al ejercicio de la acción de tutela específica o de Hábeas Data, se podrá impetrar por parte de la persona concernida y/o afectada con los datos o informaciones inexactos, incompletos, erróneos, “antiguos”, falsos o contrarios al ordenamiento jurídico vigente, cuando se persigue la actualización y rectificación de los mismos. En efecto, se interesado o afectado con los datos personales, podrá hacer uso del Hábeas Data administrativo si estima que más viable y expedito que el Hábeas Data jurisdiccional. Sin embargo, como profundizaremos más adelante al comentar los tipos de Hábeas Data en la doctrina, se ha impuesto en la praxis colombiana que la acción de tutela es la seleccionada por los colombianos para proteger y defender los derechos fundamentales incluidas las facultades del Hábeas Data de conocimiento, acceso, actualización y rectificación de la información o datos personales y se justifica como lo exige el Reglamento de la acción de tutela, que ésta se emplea como “mecanismo transitorio para evitar un daño irreparable” pese a existir otros mecanismos jurisdiccionales con igual finalidad ^[29].

En el inciso 2º del artículo 15, constitucional se refiere a las etapas o fases del tratamiento o procesamiento de datos, sean éstas realizadas con medios mecánicos o escritos, o bien con medios informáticos (electrónicos o telemáticos). Estas fases son: *la recolección,*

(29) “LA TUTELA COMO MECANISMO TRANSITORIO. Aún cuando el afectado disponga de otro medio de defensa judicial, la acción de tutela procederá cuando se utilice como mecanismo transitorio para evitar un perjuicio irremediable. / En el caso del inciso anterior, el juez señalará expresamente en la sentencia que su orden permanecerá vigente sólo durante el término que la autoridad judicial competente utilice para decidir de fondo sobre la acción instaurada por el afectado. / En todo caso el afectado deberá ejercer dicha acción en un término máximo de cuatro (4) meses a partir del fallo de tutela. Si no la instaura, cesarán los efectos de este. / Cuando se utilice como mecanismo transitorio para evitar un daño irreparable, la acción de tutela también podrá ejercerse conjuntamente con la acción de nulidad y de las demás procedentes ante la jurisdicción de lo contencioso administrativo. En estos casos, el juez si lo estima procedente podrá ordenar que no se aplique el acto particular respecto de la situación jurídica concreta cuya protección se solicita, mientras dure el proceso” (Artículo 8º del Decreto 2591 de 1991).

tratamiento y circulación de datos, en las cuales como lo enfatiza la Constitución, se respetarán la libertad y demás garantías consagradas en la Constitución.

En el transcurso del tratamiento o procesamiento de datos personales, como profundizaremos *ut infra*, son viables el Hábeas Data administrativo como el Hábeas Data jurisdiccional y aquí con mayor razón, ya que son en éstas fases del tratamiento de datos donde se presenta la alta tensión, vulnerabilidad y/o defensabilidad y protección de los derechos y libertades fundamentales de la persona.

Cuando el artículo 20 constitucional, *garantiza a toda persona la libertad... de informar y recibir información veraz e imparcial...* está garantizando un derecho universal ^[30] y un derecho incorporado al derecho nativo mediante las Ley 74 de 1968, por el cual se aprueba el Pacto internacional de derechos civiles y políticos y la Ley 16 de 1972, por el cual se aprueba el Convenio Americano sobre derechos Humanos o Pacto de San José de Costa Rica. En los artículos 19 y 13, respectivamente, se recogen el derecho, los deberes y las responsabilidades del Estado y los particulares respecto al derecho a la información, entendido éste en el más amplio sentido y no solamente en la especie aplicable al derecho periodístico, de “prensa” o de “impresión”. Se garantiza las dos visiones del derecho a la información: la activa de informar veraz, oportuna, completa y libre de errores o limitante o restricción alguna, salvo la estipulada en la Constitución y la ley y en cabeza del Estado o sus entidades, organismos o dependencias o de los particulares con función o servicio público; así como la visión pasiva de recibir información veraz, completa, imparcial, oportuna, eficaz y libre de limitantes y restricciones que no sean las autorizadas por el ordenamiento jurídico vigente.

Finalmente, el artículo 74, garantiza a *todas las personas* el derecho que ostentan *para acceder a los documentos públicos*, que interesen o afecte un derecho o libertad fundamental de una persona natural o jurídica y se hayan recabado en un banco de datos o archivo de una entidad pública o privada con función pública, o bien cuando dichos documentos estén involucrados en una cualquiera de las fases del tratamiento de datos personales.

El derecho de acceso a la información pública cualquiera sea la forma del almacenamiento o del tratamiento (mecánico, escrito o electrónico), garantizado a toda persona natural o jurídica se encuentra reglamentado con carácter pre y post constitucional a 1991, en la Ley 4 de 1913, artículo 32; en Ley 57 de 1985 o “Estatuto de la Información”, el C.C.A.; la Ley 527 de 1999 (acceso electrónico a documentos o páginas de WEB públicos y privados) y la Ley 962 de 2005 o “Estatuto Antitrámites” en Colombia.

La acción de tutela específica de Hábeas Data en Colombia desde su instauración en la Constitución de 1991, como segundo Estado de Latinoamérica e instituir y elevarla a rango constitucional, ha provocado en buena hora, un amplio y fructífero trabajo jurisprudencial de la Corte Constitucional como un mesurada labor de la doctrina especializada en pro de la estructuración, desarrollo, alcances, efectos jurídicos materiales y sustanciales y la evolución de la institución jurídico constitucional del Hábeas Data, tal como lo demostramos a lo largo de este ensayo jurídico. Todo por cuanto, en

(30) El artículo 19 de la *Declaración Universal de los derechos Humanos* de 10 de Diciembre de 1948, por el cual “Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión”.

nuestro país todavía no nace a la luz pública una ley que regule integralmente el derecho y garantía constitucional del Hábeas Data.

El Congreso de la República desde antes de la Constitución de 1991 y con mayor razón después de ésta ha avocado el conocimiento de diversos proyectos de ley ordinaria y de ley estatutaria que persiguen regular sectorial o parcialmente el derecho de Hábeas Data, sobre todo en algunas fases del tratamiento informatizado o no de datos personales, con énfasis en el dato financiero de carácter comercial, bancario, tributario y tarifario o de servicios públicos domiciliarios.

La demora mayor en Latinoamérica en reglamentar el Hábeas Data en Colombia desde 1991 hasta Diciembre de 2008 (17 años), estimamos se ha debido a que el titular del Hábeas Data, no ha sentido en sumo grado, la ausencia de una legislación específica que lo regule, porque la Constitución enlistó *númerus clausus* los derechos fundamentales que no requerían reglamentación legal para poder hacer uso de ellos en forma y aplicación directa y dentro de éstos estaba el derecho de Hábeas Data.

Además, estimamos se debe a la decida y fructífera labor de los jueces, autoridades judiciales, tribunales y Corte Constitucional en el ámbito de la jurisdicción constitucional, al resolver problemas sociales, políticos, culturales y mayoritariamente financieros que tenían las personas en nuestro país con relación al tratamiento de datos personales informatizados o no ^[31] en sus diferentes fases (recolección, selección, almacenamiento, registro, uso y comunicación ^[32]), han permitido efectivizar, estructurar y evolucionar dinámicamente el Hábeas Data, más que si aplicáramos una ley sectorial pétrea acerca de éste derecho.

-
- (31) El tratamiento de datos, no solo se refiere al tratamiento informatizado por medios electrónicos o informáticos, sino al tratamiento o procesamiento de datos en forma escrita, mecánica o manual. Tratamiento ancestral de datos, informaciones de todo tipo (incluidas las referidas a la persona) o documentos en archivos públicos y privados que requieren de un procedimiento, tratamiento o procesamiento manual que algunos llaman archivística general o especializada, bibliotecología, etc., pero al fin y al cabo, constituye un procesamiento de información que incluye etapas, que hoy a partir de la información electrónica y la creación de bases, ficheros o bancos de datos, se han evidenciado al máximo, a tal punto que se identifican por fases: recolección, selección, almacenamiento, registro y uso y comunicación. Si bien hoy por hoy, la información electrónica es mayor, más rápida en su procesamiento y utilización, más fugaz o más perenne, según el caso; que ocupa menos espacio y se almacena en medios y aparatos más ínfimamente más pequeños que los utilizados para la información tradicional, no hay duda que ésta ha generado mayores expectativas, sensibilidad, vulnerabilidad e instrumentos de defensabilidad y protección que la información tradicional o escrita; entre otras razones, porque el surgimiento de las nuevas tecnologías de la información y la comunicación (medios TIC), de la informática jurídica y de la alta porosidad y campos de penetración o intrusión que tiene el llamado "poder informático", y sobre todo la utilización abusiva, ilegítima o no conforme al derecho de estos medios electrónicos. Pese a todo, quien estime, como lo hace nuestro colega y coterráneo CIFUENTES MUÑOZ, que el Hábeas Data nació como institución jurídica y sólo es aplicable a la información o datos informatizados, es decir sometidos a procesamiento por medios electrónicos, telemáticos o informáticos, desconoce la esencia del derecho y garantía fundamental del Hábeas Data. Véase la postura del autor cuestionado en: CIFUENTES MUÑOZ, Eduardo. **El Hábeas Data en Colombia**. Revista *Ius et Praxis*, Año 3, Número 1º, Facultad de ciencias jurídicas y sociales, Universidad de TALCA, Talca (Chile), p. 81-106
- (32) RIASCOS GOMEZ, Libardo. **El tratamiento de datos personales en el derecho colombiano y comparado**. Digitocomputarizado, Universidad de Nariño, Pasto, 2002, p.15 y ss.

La Institución jurídico constitucional del Hábeas Data en Colombia, hoy por hoy y a pesar de haberse expedido la Ley 1266 de Diciembre 28 de 2008, relativa al Hábeas Data Financiero, sigue siendo una acción de tutela específica, pues la mencionada ley estima varias formas de defensa para el titular de los datos financieros, tanto en vía administrativa como en vía jurisdiccional. Dentro de ésta última vía, se propone el ejercicio de la acción de tutela ante las autoridades constitucionales competentes mediante el procedimiento breve y sumario previsto en el artículo 86, constitucional, el Decreto 2591 de 1991 y la Ley 1266 de 2008. En tal virtud, se empleará el Hábeas Data jurisdiccional en acción de tutela. Esta tendrá las siguientes connotaciones: (i) La acción de tutela puede ejercerla toda persona que vea amenazado o vulnerado algún derecho o libertad fundamental; (ii) El Hábeas Data por la ubicación orgánica, denominación y clasificación en la Constitución *ab initio*, es un derecho fundamental ^[33], a tenor del artículo 86, constitucional; (iii) Es un derecho de aplicación inmediata, según el artículo 86, es decir, “que no requiere previo desarrollo legislativo o de algún tipo de reglamentación legal o administrativa para su eficacia directa y que no contemplan condiciones para su ejercicio en el tiempo, de modo que son exigibles en forma directa e inmediata” ^[34]; (iv) Como derecho fundamental el Hábeas Data, sí el legislador decide reglamentarlo sólo deberá hacerlo mediante una ley estatutaria (artículo 152-1, constitucional), cuya aprobación, modificación o derogación exigirá de la mayoría absoluta de los miembros del Congreso y deberá efectuarse dentro de una sola legislatura, según el artículo 153 *ibid*. Además, requerirá del control de constitucional previo y automático de la Corte Constitucional sobre la exequibilidad del proyecto. Se aclara *in fine* del artículo citado que “cualquier ciudadano podrá intervenir para defenderla o impugnarla” ^[35]; (v) Es ejercita para garantizar y proteger los derechos fundamentales, incluidos la intimidad, el buen nombre, el honor, la información, el libre desarrollo de la personalidad, contra toda amenaza o vulneración por acción u omisión de las “autoridades públicas”; (vi) La protección efectiva de la tutela consistirá en la orden judicial que imparta el juez constitucional mediante sentencia para que el funcionario o autoridad pública actúe o se abstenga de hacerlo; (vii) La acción procederá cuando el interesado o perjudicado no disponga de otro medio judicial, salvo que se utilice como un mecanismo transitorio para evitar un perjuicio irremediable; y, (viii) El Hábeas Data origina un procedimiento sumario y preferente y sin mayores formalidades o ritualidades, adelantado a voluntad por la persona concernida o por quien lo represente.

2.1.5. El Hábeas Data en la Constitución Ecuatoriana de 1998, es una acción de amparo específico de carácter jurisdiccional

El Hábeas Data en la Constitución Ecuatoriana de 1998, es una acción de amparo específico de carácter jurisdiccional, por la cual toda persona podrá acceder a los datos

(33) “El derecho fundamental al habeas data, es aquel que otorga la facultad al titular de datos personales, de exigir a las administradoras de datos personales el acceso, inclusión, exclusión, corrección, adición y actualización, y certificación de los datos, así como la limitación en la posibilidades de divulgación, publicación o cesión de los mismos, conforme a los principios que informan el proceso de administración de bases de datos personales”. Sentencia T-279 de 2002 de la Corte Constitucional.

(34) Sentencia T-002-1992 de la Corte Constitucional

(35) Varios proyectos de ley ordinaria (cuando debieron ser por ley Estatutaria) sobre el Hábeas Data se expidieron posteriormente a la Constitución de 1991 y aún hasta antes de la Sentencia C-008-1995, fueron declarados inconstitucionales, como sucedió con los proyectos No. 127/93 de la Cámara y No. 12 /93 del Senado, relativos a las fases del tratamiento de datos financiero, por no seguir el trámite especial de ley estatutaria, permitió vislumbrar el carácter de derecho fundamental regulado por ley estatutaria que el Hábeas Data tiene.

que le conciernen, así como solicitar su actualización, rectificación, eliminación o anulación, si fueren erróneos o afectaren ilegítimamente sus derechos.

En el inciso 1º del artículo 94 de la Constitución de la República del Ecuador de 1998, el Hábeas Data es un derecho fundamental por el cual se garantiza a toda persona natural o jurídica, el acceso a la información pública o privada, en los siguientes términos: *“Toda persona tendrá 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 a conocer el uso que se haga de ellos y su propósito.”*

En el Inciso 2º, se garantiza otras esenciales facultades o componentes del Hábeas Data, cuando se faculta al concernido con los datos personales, para *“solicitar ante el funcionario respectivo, la actualización de los datos o su rectificación, eliminación o anulación, si fueren erróneos o afectaren ilegítimamente sus derechos”.*

El constituyente ecuatoriano, va más allá de garantizar el Hábeas Data pleno (conocimiento, acceso, actualización, rectificación y eliminación de datos personales), cuando en el inciso 3º faculta al interesado o afectado con el tratamiento de datos, para que pueda éste, *“Si la falta de atención causare perjuicio,... podrá demandar indemnización”.*

En el inciso 4º, la Constitución del Ecuador establece el procedimiento generado por la acción de Hábeas Data y el que le corresponde a datos especiales o categorizados, al sostener: *La ley establecerá un procedimiento especial para acceder a los datos personales que consten en los archivos relacionados con la defensa nacional’.* En cuanto al procedimiento de Hábeas Data de conformidad con el artículo 95 de la Constitución que describe el objetivo y fines de la acción de amparo, se aclara que ésta servirá para garantizar y “cualquier derecho” previsto en la Constitución dentro de los cuales está el de Hábeas Data del artículo 94. En consecuencia, el procedimiento utilizado para instaurar el Hábeas data será la acción de amparo especializada en la protección del tratamiento de los datos o Hábeas Data.

En el derecho ecuatoriano, se regula en la misma norma constitucional dos derechos fundamentales, a saber: a) El derecho de acceso a la información pública y privada; y b) El derecho fundamental de Hábeas Data.

El primero está amplia y detalladamente regulado en la Ley de Transparencia y acceso a la información pública de 2004 y en la Ley de Procedimiento Administrativo Ecuatoriano. El segundo, todavía aún no se ha reglamentado en la una ley correspondiente, aunque como en el caso colombiano, existen variopintos proyectos de regulación del Hábeas Data.

Uno de los últimos anteproyectos preparados desde 2006 por *La Asociación Ecuatoriana de Derecho Informático y Telecomunicaciones, AEDIT* ^[36] para ser presentado al órgano

(36) El anteproyecto como lo reconocen los autores de la AEDIT está basado en normas comunitarias europeas (Directivas comunitarias sobre datos personales y la transferencia o comunicación internacional de los mismos) y especialmente en la Ley de Protección de datos de carácter particular española de 1999 o LOPDPE. Con lo cual si el anteproyecto se convierte en proyecto legislativo y éste previos los trámites legislativos en ley de la República, Ecuador tendrá una Ley de Protección de datos Ecuatoriana LPDPE, al estilo de la Ley Argentina en Suramérica y la Española en Europa.

legislativo ecuatoriano, pretendía reglamentar el Hábeas Data para “*garantizar y proteger los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, tanto públicos como privados, 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 la Constitución Política de la República del Ecuador*”.

En el ámbito constitucional ecuatoriano la acción de amparo específica de Hábeas Data tiene alcances potenciados diferentes a los establecidos en los demás países Latinoamericanos e incluso a los países europeos. En efecto, el Hábeas data jurisdiccional ecuatoriano, no solo se extiende a solicitar ante el funcionario respectivo, la actualización de los datos o su rectificación, eliminación de los mismos, si fueren erróneos o afectaren ilegítimamente sus derechos sino también a solicitar su anulación, con lo cual el funcionario competente tendrá poderes para decretar la anulación del acto o contrato público o privado que contenga datos personales del interesado o afectado con la concreción de una base de datos o de un tratamiento informatizado o no de datos. Igualmente podrá decretar como medida cautelar la suspensión de la eficacia del acto ^[37] o contrato estatal, si fuere procedente, viable y oportuna, pues si puede lo más (anular un acto o contrato), podrá lo menos suspender temporalmente la eficacia del acto o negocio jurídico respectivo.

Igualmente, resulta potenciada la institución del Hábeas Data ecuatoriano, por parte del concernido (interesado o afectado) con los datos personales porque podrá según el inciso 3º del artículo 94, *si la falta de atención causare perjuicio a sus derechos o intereses legítimos á demandar indemnización* ante las autoridades jurisdiccionales competentes, que de seguro serán civiles, comerciales, laborales o administrativas, según fuere el caso y eventualidades de competencia de los datos personales concernidos.

2.1.6. El Hábeas Data en la Constitución centroamericana de Honduras, es una acción exhibitoria de los datos personales y familiares de carácter jurisdiccional

El Hábeas Data en la Constitución centroamericana de Honduras, es una acción exhibitoria de los datos personales y familiares de carácter jurisdiccional que se tramita en lo pertinente por el procedimiento de amparo.

En la Constitución de Honduras de 1982, en el artículo 182 (Reformado por Decreto 243/2003), eleva a rango constitucional el derecho fundamental de Hábeas Data desde la fase de acceso a la información pública y privada, y una vez conocida ésta y según las eventualidades, para solicitar su actualización, rectificación y enmienda.

En efecto, la también garantía constitucional del Hábeas Corpus regulada concomitantemente con el Hábeas Data son reconocidas por el Estado para toda persona, y ésta última, según la parte *ab initio* del artículo 182 “*únicamente puede promoverla la persona cuyos datos personales o familiares consten en los archivos, registros públicos o privados*”.

Este derecho y garantía constitucional, según el inciso 1º del numeral 2º lo ostenta “*Toda persona tiene el derecho a acceder a la información sobre sí misma o sus bienes en*

(37) RIASCOS GOMEZ, Libardo O. *Las Medidas cautelares en el procedimiento administrativo*. Tesis Doctoral, Universidad de Navarra (España), Pamplona, 1986, p. 99 y ss.

forma expedita y no onerosa, ya esté contenida en bases de datos, registros públicos o privados y, en caso de que fuere necesario, actualizarla, rectificarla y-o enmendarla”.

En el inciso 2º del numeral 2º del citado artículo, al referirse al trámite breve y expedito generado por el Hábeas Data, manifiesta que se ejercerá *“sin necesidad de poder ni de formalidad alguna, verbalmente o por escrito, utilizando cualquier medio de comunicación, en horas o días hábiles o inhábiles y libre de costas. Únicamente conocerá de la garantía del Hábeas Data la Sala de lo Constitucional de la Corte Suprema de Justicia, quien tendrá la obligación ineludible de proceder de inmediato para hacer cesar cualquier violación a los derechos del honor, intimidad personal o familiar y la propia imagen”.*

En el inciso 4º del numeral y artículo citados, advierte a los *“titulares de los órganos jurisdiccionales que dejaren de admitir estas acciones constitucionales, incurrirán en responsabilidad penal y administrativa”.*

Según el artículo 183 de la Constitución Hondureña, *“el recurso de amparo es el instrumento jurídico que se utiliza, para mantener o restituir “el goce o disfrute de los derechos o garantías que la constitución establece”, incluido el derecho y garantía constitucional de Hábeas Data.*

La institución jurídica constitucional del Hábeas data en la Constitución Hondureña se conceptualiza como un derecho fundamental que regula el uso, goce y control de los datos o informaciones personales o familiares que se recaben en *los archivos, registros públicos o privados* informatizados o no, o también si fuere del caso, para solicitar a las autoridades jurisdiccionales competentes que sean actualizados, rectificadas o “enmendados”, cuando afectaren los *derechos del honor, intimidad personal o familiar y la propia imagen* y llegado el caso, *tendrán la obligación ineludible de proceder de inmediato para hacer cesar cualquier violación.* En este último sentido el Hábeas Data se estructura además como una garantía constitucional eficaz para proteger y defender otros derechos constitucionales de igual jerarquía como son la intimidad personal y familiar de las personas y los demás enlistados en la norma constitucional.

El procedimiento de amparo del Hábeas Data Hondureño tiene reglas expresas generales y específicas en los artículos 183 y 182 de la Constitución. Las reglas específicas son: (i) El procedimiento sin mayores formalidades o ritualidades y puede iniciarlo toda persona concernida con los datos personales o familiares, sin necesidad de apoderado; (ii) Puede iniciarse en forma verbal o por escrito; (iii) La acción es atemporal y puede impetrarse en cualquier día hábil o no y está exento de costas procesales; (iv) La competencia la tiene en forma exclusiva y excluyente la Sala Constitucional de la Corte Suprema de Justicia; y, (v) Los funcionarios jurisdiccionales responderán penal y administrativamente en caso de inobservancia injustificada del mecanismo procesal y derecho fundamental del Hábeas Data.

Como se observa esta normatividad constitucional regulatoria del Hábeas Data, más parece una reglamentación de tipo legal pero que conceptualiza en forma puntual y excesiva esta institución jurídica no solo en el núcleo esencial del derecho (facultades de conocimiento, acceso, actualización, rectificación y eliminación de datos personales), sino en el procedimiento de amparo específico aplicado a éste, con lo cual tenemos un derecho y una garantía constitucional de Hábeas Data de carácter eminentemente jurisdiccional.

2.1.7. El Hábeas Data en la Constitución Peruana es una acción de amparo específico de protección de datos personales.

El Hábeas Data en la Constitución Peruana es una acción de amparo específico de protección de datos personales, la cual procede contra todo hecho u omisión del Estado o de los particulares cuando amenace o vulnere el derecho a la información, la intimidad, la voz, la imagen, el honor y la reputación.

En la Constitución del Perú de 1993, se reglamenta en forma expresa el derecho y "garantía constitucional" del acción de habeas data en el artículo 200 numeral 3º de la siguiente forma: "Son garantías constitucionales: ... 3º *La Acción de Hábeas 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 5, 6, y 7 de la Constitución*".

Por su parte el artículo 2º en los incisos 5º al 7º del mencionado artículo 200, sostiene: "toda persona tiene derecho a: (...)

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 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.

6. A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y 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.

Toda persona afectada por afirmaciones inexactas o agraviada en cualquier medio de comunicación social tiene derecho a que éste se rectifique en forma gratuita, inmediata y proporcional, sin perjuicio de las responsabilidades de ley.

Son garantías constitucionales, las acciones de hábeas Corpus, amparo, hábeas data, cumplimiento, inconstitucionalidad y popular.

La Constitución peruana conceptualiza el Hábeas Data en forma amplia, a partir del objeto y finalidad de la Institución, de la relación *numerus clausus* de los derechos fundamentales protegidos y de las excepciones a la aplicación de la garantía constitucional del Hábeas Data. Sin embargo, la Constitución no hace referencia expresa e integral al núcleo esencial del Hábeas Data en las facultades o derechos de toda persona a solicitar la corrección, la actualización y eliminación de los datos personales, aunque sí lo hace si lo hace sobre el derecho de acceso y conocimiento de la información por remisión del artículo 200-3º al artículo 2-5º de la Constitución. También hace referencia expresa a la facultad que tiene la persona concernida con los datos o informaciones personales de rectificación e impedimento de comunicación de los mismos cuando los datos sean inexactos o agraviantes.

La acción y garantía constitucional del Hábeas data peruana, se instauró como un mecanismo procedimental idóneo, para la protección y defensa de los siguientes derechos: (i) Solicitar y recibir información de una entidad pública. Se exceptúan las que afectan al derecho a la intimidad y a la seguridad nacional; así mismo las que se refieren al secreto bancario y la reserva tributaria; (ii) "A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la

intimidad personal y familiar”; (iii) “Al honor y a la buena reputación, a la intimidad personal y familiar así como a la voz y a la imagen propias”; y (iv) A la rectificación en forma gratuita, inmediata y proporcional, cuando la persona afecta reciba “*afirmaciones inexactas o agraviada en cualquier medio de comunicación social... sin perjuicio de las responsabilidades de ley*”. En síntesis, la acción de Hábeas Data garantiza y protege el derecho acceso, conocimiento y rectificación de la información pública y privada.

El Perú, es el único Estado Latinoamericano que ha regulado en el año 2004 (Ley No. 28.237 de 31 de Mayo), un procedimiento constitucional único de amparo, con algunas peculiaridades para las llamadas garantías constitucionales de Hábeas Corpus, Hábeas Data, cumplimiento, inconstitucionalidad y popular. El Código Procesal Constitucional del Perú compila las normas procedimentales de las acciones y garantías constitucionales de forma tal que facilitan la labor de búsqueda y aplicabilidad de las normas referidas a éstas por parte del operador jurídico y las autoridades judiciales, pero a la vez simplifican los cuerpos normativos de índole eminentemente procesal en un Códex que antes que otra cosa resulta práctico y exento de repeticiones o contradicciones normativas, que suele suceder cuando se regula una misma materia.

Por lo anteriormente expuesto, algunos tratadistas del derecho público peruano, manifiestan que el Hábeas Data en aquél país no solo es una acción y garantía constitucional sino un auténtico procedimiento constitucional ^[38]. Denominación doctrinal que tiene serios reparos, pues la acción no puede ser a la vez la totalidad jurídica a la que le sirve de inicio, es el motor esencial del procedimiento, pero no lo es todo; la parte no puede ser el todo. Está bien que se nomine indistintamente al Hábeas como acción, garantía, recurso e incluso derecho fundamental, pero no como procedimiento *per se*. Cosa diferente es que digamos que el Hábeas Data origina un procedimiento específico que lo podremos intitular como procedimiento constitucional de Hábeas Data, pero no que el Hábeas Data es un proceso en sí mismo ^[39].

2.1.8. En la Constitución española, se limita “la informática” para proteger el pleno ejercicio de derechos, principalmente el de la intimidad y el honor de las personas.

En la Constitución española, se limita “la informática” para proteger el pleno ejercicio de derechos, principalmente el de la intimidad y el honor de las personas. El legislador con base en esto regula la acción de protección de datos de la persona humana y que el Tribunal Constitucional en sus providencias y la doctrina en sus tratados asimila en su constitución, desarrollo y efectos jurídicos sustantivos y materiales a la acción de Hábeas Data latinoamericana.

Como prototipo de las Constituciones europeas, hemos tomado la Constitución Española de Diciembre 28 de 1978 o CE, a fin de conceptualizar por vía de interpretación y asimilación de instituciones jurídico-procesales, el que podríamos llamar el Hábeas Data europeo. En efecto, en Europa ni siquiera en la Constitución Alemana, Suiza y Austriaca de la década de los setenta, donde comenzaron por vez primera a expedirse normas

(38) Vid. EQUIGUREN, Francisco. *El Hábeas Data y su desarrollo en el Perú*. Revista *Ius et Práxis*, Año 3, Facultad de ciencias jurídicas y sociales, Universidad de Talca, Talca (Chile), p.119.

(39) Así parece entenderlo otro tratadista, docente universitario y amigo peruano, TORRES CASTRO, Carlos A. *Código Procesal Constitucional*. Estudio preliminar, 1ª ed., Sociedad de Estudios para una cultura de paz, Lima (Perú), Noviembre 30 de 2004, p.48-49

protectoras de los derechos fundamentales, principalmente de la privacidad (“The privacy” anglosajona, o en nuestro lenguaje actual el derecho a la intimidad) frente a los abusos o excesos del tratamiento de datos por medios informáticos; como tampoco, en las Constituciones de Portugal de 1976 ni en la Constitución Española de 1978, se hace referencia a la Institución jurídica de origen latino del Hábeas Data, menos aún en las respectivas legislaciones que reglamentaron la Constitución portuguesa y española.

En las constituciones y legislación europeas la institución procesal idónea para proteger los derechos y libertades fundamentales de los posibles abusos o excesos de la informática (Artículo 35 de la Constitución Portuguesa ^[40] y artículo 18-4 de la CE) es la acción de protección de datos que cumple idénticos fines, objetivos y efectos jurídicos al del Hábeas Data latinoamericano. Por eso, ha sido tarea de los Tribunales Constitucionales ^[41] y de la doctrina especializada ^[42] europea la asimilación u homologación jurídica en todos sus extremos de la acción de protección de datos de la persona humana (exclusiva y excluyentemente ^[43]) con la acción, recurso o garantía constitucional de Hábeas Data que procede para proteger los datos personales no sólo de las personas humanas o físicas, sino también por vía de interpretación jurisprudencial, en unos Estados o por vía normativa expresa en la Constitución o leyes reglamentarias en otros Estados latinoamericanos.

El artículo 18-4 de la CE estipula: “*La ley limitará el uso de la informática para garantizar*

-
- (40) 35-1. Todos los ciudadanos tendrán derecho a tener conocimiento de lo que consta en forma de registros informáticos que les conciernen y de la finalidad a la que se destinan esas informaciones (datos o registros), y podrá exigir, llegado el caso, la rectificación de los datos, así como su actualización. 2. Está prohibido el acceso de terceros a los ficheros (o banco de datos) con datos personales o a la respectiva interconexión de aquéllos, a través de los flujos transfronterizos, salvo en las casos exceptuados en la ley (Inciso nuevo). 3 La informática no podrá ser utilizada para el tratamiento de datos referentes a las convicciones filosóficas o políticas, a la filiación partidista o sindical, a la fe religiosa o la vida privada, salvo cuando se trata de procesamiento de datos no identificables individualmente para fines estadísticos. 4. La ley definirá el concepto de datos personales para efectos de registro informático (nuevo). 5. Se prohíbe la atribución de un número nacional único a los ciudadanos”. En: AA.VV. **Constituição Novo Texto**. Coimbra editora, Edição organizado JJ. Gomes Conotilho o vital M., 1982
- (41) Una de las sentencias del TC español prototipo sobre el particular fue la STC 254/1993, de 20 de Julio, en la cual se puede leer en el Fundamento Jurídico (FJ) número 6º, lo siguiente: “*la garantía de la intimidad adopta hoy un contenido positivo en forma de derecho de control sobre los datos relativos a la propia persona. La llamada ‘libertad informática’ es, así también, derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data)*”. Nótese que el Tribunal Constitucional ibérico asimila en principio el derecho a controlar los datos que le conciernen a una persona a una acción constitucional dirigida a reclamar la protección de datos personales recabados en una base, fichero o banco de datos que lo identifica con “programa informático” y éste curiosamente lo identifica con el Hábeas Data. Es entendible dicha asimilación en aquella época, pues en el derecho europeo se ha privilegiado los derechos y libertades constitucionales por encima de la acción idónea para proteger y defenderlos y obviamente también por encima del mecanismo que amenaza o vulnera los derechos a la intimidad y el honor de los “ciudadanos”, cual es la “informática”.
- (42) Entre muchos otros: FAIREN GUILLEN, Víctor. **El Hábeas Data y su protección actual surgida en la Ley española de Informática del 29 de Octubre (Interdictos, Hábeas Corpus) –Primera Parte—** En: Revista de Derecho procesal. R.D.P. No. 3º, Madrid, 1996; CASTELLS ARTECHE, José M. **La Intimidad informática**. En: Estudios sobre la Constitución Española en homenaje al profesor Eduardo García de Enterría. Ed. Civitas, Tomo II, Madrid, 1991. P. 12; GONZALEZ NAVARRO, Francisco. **Comentarios a la ley de Régimen Jurídico de las administraciones públicas y procedimiento administrativo común (Ley30/92)**. Ed. Civitas S.A., Madrid, 1997, p. 697-698; LOPEZ MARTINEZ, Juan. **La protección de los datos y la información en poder de la Hacienda Pública**. Profesor de Derecho financiero y tributario. Vía Internet, 2007.
- (43) La Ley Núm. 30 de 26 de Noviembre de 1992, relativa al “Procedimiento Administrativo Español”, regula el derecho de acceso a Archivos y registros informatizados o no que se hallan recabados por las personas jurídicas de derecho público las Administraciones Públicas.

el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos”.

El artículo 18-4 CE, se ha considerado el fundamento constitucional garantista del Estado Español, cuando se trata de derivar el cúmulo de derechos fundamentales que tienen que ser protegidos contra cualquier agresión efectiva o potencial que pueda ocasionarse tras “*el uso de la informática*” en forma abusiva o contraria al ordenamiento jurídico vigente. Por ello, en forma explícita y terminante la Constitución de España, prevé que la limitación del uso de la informática para garantizar los derechos y libertades constitucionales e incluso los enlista *numerus clausus*. Quizá por ello, la jurisprudencia y doctrina españolas de la década de los noventa estudió el fenómeno de la informática como una potencial amenaza o vulneración efectiva del pleno ejercicio de los derechos fundamentales y particularmente del derecho a la intimidad ^[44], no se reparó en que los avances de las nuevas tecnologías de la información y la comunicación (TIC) apoyadas o potenciadas por los medios electrónicos, telemáticos o informáticos, *per se* no genera peligro o vulnerabilidad a los derechos, es el uso defectuoso, irregular, impreciso, indebido e ilegal el que genera transgresión de los derechos y libertades de las personas.

De hecho, las leyes post-constitucionales a 1978 de carácter civil, administrativo y penal que protegían entre otros derechos, el derecho a la intimidad de las personas en España, como la Ley Orgánica No. 1 de 1982, de 5 de Mayo, relativa a la “protección civil del derecho al honor, la intimidad personal y la propia imagen”, luego la L.O. 5/1992, Octubre 29, “*Ley Orgánica de regulación del tratamiento automatizado de datos de carácter personal*”; la Ley Orgánica No.15 de Diciembre 23 de 1999 o LOPDP que algunos la denominan como la “nueva LORTAD”^[45] y el Código Penal de 1995 ^[46], regulan el uso

(44) (45) LOPEZ MARTINEZ, Juan. **La protección de los datos...** *Ob., ut supra cit.*

(46) Es de destacar en el derecho penal español la cuidadosa como compleja redacción de normas que tipifican delitos contra la intimidad y la propia imagen (no así el honor), como derechos fundamentales altamente protegidos en los art. 18.4, 20.1.d) y 105 CE, contra las injerencias de la informática. En efecto, el Título X, *De los delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad de domicilio* (arts. 197 a 204) del C.P., del 95, y considera que la *privacy*, “libertad informática” en el art. 197.2, tipifica un elenco de conductas que comportan “abusos informáticos”, aunque no en forma completa, pero sí más coherente en la descripción de conductas típicas codificadas y en forma cerrada. No es completa, porque el art. 197.1, recoge las conductas de interceptación, grabación o reproducción electrónica ilícita de comunicaciones informáticas (mensajes de correo electrónico). Igual la captación subrepticia de mensajes de correspondencia electrónica y el apoderamiento físico subrepticio, con la intención de descubrir la intimidad ajena de mensajes de correspondencia informática ya impresos fuera del sistema. El art.197.2, en su redacción final es sustancialmente mejor que la presentada en el proyecto de Código Penal de 1992 (art.198.2) y del proyecto de C.P. de 1994 (art.188.2), textos en los que se tipificaba únicamente el apoderamiento no autorizado de datos personales. El mentado artículo es una norma cerrada, pues antes que la técnica de tipificación de conductas de ley penal en blanco se escogió la de la codificación y describir las conductas delictivas en forma cerrada para incriminar los delitos contra el *habeas data* o *libertad informática*. Técnica que suscita problemas a la hora de esclarecer las conductas y evidente incorrección en la definición técnica de las conductas típicas, pues para ello hay que recurrir a la LORTAD y otras normas extrapenales que informan las conductas penales previstas en el art. 197.2., como el Convenio de 28 de Enero de 1981 del Consejo de Europa y la Directiva 95/45/CE, del Parlamento y el Consejo de Europa, que completa y amplía la protección del Convenio sobre las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Las conductas típicas previstas en el art. 197.2. CP. del 95, son: a) En el inciso primero, quedan tipificadas las acciones de apoderamiento, utilización o modificación de datos reservados de carácter personal, que se hayan automatizados de forma electrónica o que obren en cualquier otro tipo de archivo o registro público o privado. Estas acciones deben realizarse *sin autorización* y *en perjuicio de tercero*; b) En inciso segundo, se tipifica la acción de acceder por cualquier medio a los datos personales y a quien los altere o utilice en perjuicio del titular o de un tercero. Vid. RIASCOS GOMEZ, Libardo O. **El derecho a la intimidad, la visión ius-informática y los delitos relativos a los datos personales.** Tesis Doctoral, Universidad de Lleida (España), Lleida, 1999, p. 505 y ss.

abusivo o ilegal de la informática, a efectos de demostrar que es éste uso indebido o contrario al ordenamiento jurídico el que abre el gran portal de las amenazas o vulneraciones al pleno ejercicio de los derechos de la persona. Por ello, aún en las normas de carácter civil y administrativo, se regulan las indebidas injerencias a los derechos constitucionales y legales, las “infracciones administrativas” y las correspondientes sanciones previo procedimiento idóneo. El Código Penal obviamente regula los delitos contra la intimidad de las personas.

En consecuencia, son las leyes protectoras de datos personales de índole civil y administrativo, la que al reglamentar el artículo 18-4 de la CE, las que conceptualizan a la acción de protección de datos personales, cuando estructuran, desarrollan e incluso potencian el tratamiento informatizado o no de protección de datos personales y la correspondiente acción para hacerlo efectivo e idónea en la protección y garantía de los derechos y libertades constitucionales, pero principalmente el derecho a la intimidad y la buena imagen. De contera, la LORTAD y la LOPDP, son las que se encargan de conceptualizar y estructurar integralmente la acción de protección de datos; el tratamiento informatizado o no de datos; los principios, limitaciones y restricciones que rigen en el tratamiento de datos, la categorización de datos personales (anodinos, normales, sensibles y ultrasensibles) y las normas reguladoras de los bancos de datos de titularidad pública y de titularidad privada.

2.2. Conceptualización del Hábeas Data en el ámbito legislativo

Se conceptualiza la Institución jurídica del Hábeas data en las leyes latinoamericanas que regulan sobre lo siguiente: (i) la Protección de los Datos personales, como es el caso la Nación de Argentina y varias de sus provincias con autonomía legislativa, como la de Neuquen y en la ciudad capital de Buenos Aires en el año de 2000; (ii) además de reglamentar la protección de los datos personales lo hacen sobre “la vida privada”, como en Chile en el año de 1999; o bien, los “datos financieros”, como en el caso de Uruguay en el año 2004 y Colombia en 2008; (iii) la Transparencia en las gestiones Públicas y el acceso a la información pública, como es el caso de Panamá en el año 2002; y, (iv) la reglamentación codificada de varias acciones o garantías constitucionales compiladas en un Código Procesal Constitucional, como es el caso exclusivo del Perú en el año 2002;

La conceptualización del Hábeas Data latinoamericano tiene un común denominador en el objetivo y finalidad de la misma, pero varía levemente cuando se trata de particularidades o especificidades aplicables al procedimiento que genera el Hábeas Data, bien sea éste denominado de amparo específico, como pasa en la gran mayoría de Estados latinoamericanos, o bien cuando se lo nombra como proceso exclusivo de Hábeas Data, que es la excepción. Esas especificidades de adición o cambio de nombre de las facultades del Hábeas Data, o bien de carácter técnica o procedimental las anotaremos al margen.

No sobra advertir que la constitucionalización del Hábeas Data en América latina comenzó a finales de la década de los ochenta con la Constitución Brasileña de 1988 y continuó en la década de los noventa: Colombia en 1991, Paraguay en 1992, Perú en 1993, Argentina 1994, Ecuador 1998, Venezuela en 1999 y prosigue en la década del 2000, con Panamá, Honduras, Bolivia, entre otros. Sin embargo, la reglamentación legislativa del Hábeas Data, ha demorado 4, 8, 12 o 17 años (como en el caso de Colombia) por variopintas razones sociales, económicas, culturales, por la mayor efectividad y garantía deparada por los jueces y tribunales en sus providencias de tutela (en Colombia) e incluso por eventualidades políticas internas de los Estados y hasta por la

advertida limitación, restricción o prohibición a tocar con el Hábeas Data, el “sacro-santo” secreto o sigilo profesional periodístico, la seguridad del Estado y el derecho a la intimidad (o privacidad como siguen nominándola en algunas leyes latinas) de las personas.

En tal virtud, las Leyes Latinoamericanas conceptualizan al Hábeas Data siguiendo los parámetros de un común denominador para todas, aunque se denominen acción, recurso o garantía de Hábeas Data.

Esta acción, recurso o garantía legislativa es de carácter jurisdiccional y tiene como objetivo y finalidad primordial la protección y garantía de los derechos constitucionales y legales, especialmente el derecho a la intimidad, el honor, el buen nombre, la imagen, la voz, la información y la reputación, siempre que los datos o informaciones personales se hayan tratados o procesados por medios informáticos, medios manuales o escritos y se hayan recabado en bancos o bases de datos. El derecho de Hábeas data protege desde el acceso y conocimiento de los datos personales hasta la actualización, rectificación y eliminación de éstos, cuando resultan inexactos, erróneos, incompletos, “antiguos”, “discriminatorios”, falsos o contrarios al derecho.

Las especificidades en algunas las leyes latinoamericanas son las siguientes:

2.2.1. En La Ley No. 25.326 de Octubre 4 de 2000 de la República Argentina o LPDA, el Hábeas Data es una acción de amparo específico de ámbito jurisdiccional.

En la Ley No. 25.326 de Octubre 4 de 2000 de la República Argentina o LPDA, el Hábeas Data es una acción de amparo específico de ámbito jurisdiccional y protege en forma integral los datos personales de la persona natural y jurídica o de “existencia ideal”.

La Ley No. 25.326 de Octubre 4 de 2000 de la República Argentina (LPDA), relativa a las “Disposiciones generales, principios generales relativos a la protección de datos, derechos de los titulares, usuarios y responsables de archivos, registros y bancos de datos. Control. Sanciones. Acción de protección de los datos personales”, 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 la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre”*.

Dentro de los derechos de los titulares de los datos, relaciona el derecho acceso y conocimiento de la información y los derechos de rectificación, actualización y supresión. Sobre éste último que lo asimila a eliminación, aclara en el artículo 16-5º de la LPDA, que *“no procede cuando pudiese causar perjuicios a derechos o intereses legítimos de terceros, o cuando existiera una obligación legal de conservar los datos”*. Así mismo adiciona una facultad más al Hábeas Data en el artículo 33, al decir que la persona concernida también podrá solicitar la “confidencialidad” de los datos en los términos previstos en la ley.

En consecuencia, la conceptualización del Hábeas Data Argentino regula una acción de amparo específico de carácter jurisdiccional que tiene un objeto y finalidad integral de protección del tratamiento de datos personales y que adiciona a las facultades tradicionales del Hábeas Data, los derechos de confidencialidad y supresión de los datos, pero éste último proscrito si con ello se pretende causar perjuicio a terceras personas o se vulnera la fase de conservación de algunos datos protegidos por la ley.

El procedimiento jurisdiccional de amparo específico (“juicio sumarísimo”) de Hábeas Data Argentino se rige por la LPDA de 2000 y las normas del Código Procesal Civil y Comercial, por remisión normativa prevista en el artículo 37.

2.2.2. En la Ley No. 19.628 de Agosto 28 de 1999 de Chile, es una acción jurisdiccional ejercitable previo agotamiento de una vía administrativa.

En la Ley No. 19.628 de Agosto 28 de 1999 de Chile o “*Ley sobre Protección de la vida privada o protección de datos de carácter personal*”, es una acción jurisdiccional ejercitable previo agotamiento de una vía administrativa y protege los derechos fundamentales, principalmente la privacidad o intimidad de las personas.

En la ley Chilena se privilegia la protección de “The privacy” anglosajona (o derecho a la intimidad) y por tanto se regula enfáticamente las fases o etapas del tratamiento informatizado o no de datos públicos y privados desde la recolección, selección, almacenamiento, registro y comunicación de datos. Sobre éste último privilegia el derecho de oposición, sobre cualquiera otro, en la fase de recolección de datos por parte del titular de los mismos, con lo cual adiciona a los tradicionales (rectificación, actualización y eliminación) el de oposición y el modificación”, si los datos son inexactos, erróneos, equívocos o incompletos en cualquier etapa del tratamiento.

La acción y procedimiento de amparo específico de Hábeas Data ante las autoridades judiciales civiles competente, solo es posible tras la negativa a contestar la petición de la información, la cancelación, el acceso o la eliminación de datos realizada por el titular, según el artículo 16 de la LPVP o PDP. En tal virtud, se establece una especie de vía previa que debe agotarse antes de hacer uso de la acción integral de Hábeas Data.

La LPVP o PDP dedica un capítulo especial a la responsabilidad diferente a la penal y administrativa de los destinatarios (usuarios y responsables de los bancos de datos) de la ley, con lo cual crea una responsabilidad patrimonial de carácter civil y/o comercial, según la naturaleza jurídica y el tratamiento del dato personal.

La conceptualización legal del Hábeas Data Chileno entonces incorpora además de ser un acción integral de carácter jurisdiccional, el agotamiento previo de una vía administrativa si las entidades, organismos o dependencias son de carácter público, o bien el agotamiento del derecho de petición ante las entidades privadas, financieras o crediticias, pues la ley Chilena lo regula como un capítulo más al dato financiero. Además habrá que decir que la acción de Hábeas data Chilena tiene también una finalidad de responsabilidad patrimonial para usuarios y responsables de los bancos de datos

2.2.3. En la Ley 6º de 22 de Enero de 2002 de Panamá, el Hábeas Data es una acción de amparo específico de carácter jurisdiccional.

En la Ley 6º de 22 de Enero de 2002 de Panamá de “transparencia en la gestión pública”: El Hábeas Data es una acción de amparo específico de carácter jurisdiccional que protege los derechos constitucionales y los datos personales y pertenece a su esencia el derecho a la información.

En la legislación panameña, la conceptualización del Hábeas Data debe además de lo dicho en la conceptualización tipo *ut supra* suministrada, prever que la Institución jurídica se hace en el ámbito de una Ley de Transparencia de la gestión pública y el acceso a la información pública y privada.

En efecto, el legislador panameño le dedica atención y regulación normativa especial al derecho a la información, a los derechos, deberes y responsabilidades del Estado y los particulares en ejercicio de suministrar y recibir información, así como enfatiza en la información confidencial y de acceso restringido.

En cuanto a la primera, relaciona la no revelación o divulgación (o “descubrimiento”, como se dice en el derecho anglosajón) de la información confidencial de las personas humanas de la que hacen parte tanto del núcleo “duro” o esencial de la intimidad, como las concernientes a la “vida privada” de las personas, a los asuntos penales, policivos, médicos, correspondencia escrita y electrónica y a las conversaciones telefónicas, entre muchas otras informaciones.

De la segunda, relaciona como información de acceso restringido, la relativa a: (i) la seguridad del Estado; (ii) los secretos comerciales; (iii) la información sobre procesos realizados por el Ministerio Público, las fuerzas militares y de policía, la Dirección de Aduanas y la Contraloría General de la Nación; (iii) información sobre yacimientos mineros y petrolíferos; (iv) información documental diplomática; (v) procesos y documentos judiciales penales y policivos; (vi) documentos e información de la Presidencia, Vicepresidencia y “gabinete” ministerial; (vii) Transcripciones y documentos de la Asamblea Legislativa.

El Procedimiento de amparo específico de Hábeas Data de carácter jurisdiccional, previsto en los artículos 17 a 19, de la Ley panameña, describe la legitimación del Hábeas Data para toda persona natural o física concernida con los datos personales. El proceso utilizado será sumario, sin formalidades y sin presencia de abogado y respecto a la sustanciación, impedimentos, notificaciones y apelaciones, se aplicarán las normas que para estas materias se regulan en el ejercicio de “*la acción de Amparo de Garantías Constitucionales*”.

En consecuencia, la conceptualización del Hábeas Data Panameño incorpora elementos de un Hábeas Data integral pero basado en el derecho constitucional a la información y dentro de ésta a la de índole pública. Más aún impone la ley un “Código de Conducta” que debe ser implementado por las entidades del Estado, si aún no lo tienen, para el “correcto ejercicio de la función pública” (artículo 27) con miras a dar aplicación integral de la ley no solo desde el punto de vista normativo o positivista sino desde la normas de “moralidad pública” libre de cualquier acto de corrupción o de ineficiencia administrativa.

2.2.4. En la Ley No. 17938 de Octubre 1º de 2004 del Uruguay, el Hábeas Data es una acción de amparo específico para proteger datos personales y principalmente los financieros.

En el caso de la República del Uruguay la conceptualización del Hábeas Data tiene un claro sabor sectorial con énfasis en el dato financiero. En efecto, la Ley No. 17938 de Octubre 1º de 2004 o “*Ley de protección de datos personales para ser utilizados en informes comerciales y el Hábeas Data*” del Uruguay (LPDP_HDU), hace énfasis en los datos personales de carácter financiero, principalmente bancario y comercial. La ley reglamenta las fases del tratamiento de datos personales (el registro, almacenamiento, distribución, transmisión, modificación, eliminación, duración), cuando estén en archivos, bases de datos, u otros “medios similares autorizados” (se entenderá en escritos, documentos tradicionales, o “informes”), sean éstos públicos o privados, “*destinados a brindar informes de carácter comercial*”. Se exceptúa en la aplicación de esta ley a los datos e informaciones de la persona humana siguientes: (i) los datos de carácter personal que se originen en el ejercicio de las libertades de emitir opinión y de informar; (ii) los

relativos a encuestas, estudios de mercado o semejantes; y, (iii) los datos sensibles sobre la privacidad de las personas.

La conceptualización de la Institución del Hábeas data en la Ley uruguaya entonces debe tener en cuenta que no es una ley integral y que por tanto es aplicable tan solo a los datos financieros de las personas, sean públicas o privadas.

Si bien la norma es la primera en el ámbito latinoamericano, estimamos que no es un prototipo normativo en la materia, pues contiene aspectos que bien pudo aprovechar para expedir un ley integral del Hábeas Data, tales como la reglamentación de las fases o etapas del tratamiento de datos, los principales principios aplicables a dichas fases y, el objetivo y finalidad de la acción de amparo específica de Hábeas Data de carácter jurisdiccional. El restante cuadro normativo, Título I, Capítulo III destinado específicamente al “*Tratamiento de datos personales relativos a las obligaciones de carácter comercial*” y previsto en los artículos 8 a 11.

2.3. En el ámbito de los proyectos de Leyes Estatutarias y en la Ley 1266 de 2008 o Ley de Habeas Data Financiero en Colombia

En los diferentes proyectos de leyes Estatutarias colombianas, a partir del año 2000 hasta el 2007, se han suministrado diferentes conceptualizaciones del Hábeas Data General o sectorial (de carácter financiero, principalmente y que a la postre fue el que prosperó porque se expidió una ley de habeas data financiero en 2008). Estos son:

2.3.1. En el proyecto de ley Estatutaria No. 071 de 2002: El Hábeas Data de carácter administrativo aplicado al dato financiero

El proyecto regulaba los “*Bancos de datos financieros o de solvencia patrimonial y crediticia...*” y supuestamente reglamentaba “*la protección integral de los datos 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...*”

La conceptualización del Hábeas Data, aunque el término no aparecía expresamente en el intitulado del proyecto ni en el contenido del proyecto, éste se infería de uno y otros aspectos. En efecto, el Hábeas Data constituía la institución jurídica idónea para proteger los datos tratados o procesados mediante medios informáticos o no, sean éstos públicos o privados y estén dirigidos a “dar informes” (tal como lo había reglamentado la Ley de protección de Datos de Argentina y la correspondiente del Uruguay) y consecuentemente garanticen los derechos fundamentales principalmente el honor y la intimidad. En este sentido el Hábeas data constituía una garantía fundamental que servía para proteger otros derechos de igual rango.

En el artículo 5º y 9º del proyecto se regulaba los derechos de los titulares de los datos personales, o dicho de otro modo, el conjunto de algunas facultades que tiene el titular del derecho de Hábeas data propio o directo de carácter administrativo, tales como: 1) El derecho de Acceso a la información; 2) El Derecho de solicitud y obtención de datos personales incluidos en bancos de datos públicos y privados, 3) El Derecho a obtener información veraz, oportuna (en el término de 10 días a la solicitud), gratuita y en forma eficiente por el responsable del banco de datos o por la fuente de información que la tenga; y, 4) El derecho a la eliminación o cancelación de datos, cuando su almacenamiento “*carezca de fundamento legal o cuando la obligación haya cesado.* El

responsable del banco de datos personales procederá a la eliminación o cancelación de los datos, sin necesidad de requerimiento del titular". Éste último derecho componente del derecho de Hábeas Data, se regulaba en forma inconexa en el artículo 9 del proyecto, significando con ello, que los demás componentes del Hábeas Data respecto de la eliminación o cancelación de datos hacían parte de éste, pero no la supresión, bloqueo o borrado electrónico de datos personales de las bases o ficheros de datos correspondiente.

2.3.2. El Proyecto de Ley Estatutaria S075 de 2002: El Hábeas Data de carácter administrativo aplicado al dato financiero

El proyecto se intitulaba: *"por el cual se desarrolla el derecho al acceso a la información financiera y comercial, así como la relacionada con el cumplimiento e incumplimiento de obligaciones fiscales, parafiscales, de servicios públicos domiciliarios y cualquiera otra que tenga utilidad pública, y se regula la actividad de administración y uso de tal información"*

En este proyecto de Ley, existen varias definiciones técnico-jurídicas aplicables a las fases o etapas del tratamiento de los datos personales y precisamente del conjunto de éstas (las cuales fueron pormenorizadamente reguladas en el proyecto) se puede deducir la conceptualización del Hábeas Data, porque al igual que el anterior proyecto, expresamente no se incluye el *nomen* de ésta.

Estos conceptos son: (i) *Administración de los bancos de datos o centrales de la información.* Es la recolección, almacenamiento, procesamiento y suministro de la información; (ii) *Acceso a la información:* Es el derecho que tienen los titulares de la información a conocer, actualizar y rectificar los registros administrados por los operadores de los bancos de datos o centrales de información; (iii) *Banco de datos o centrales de información.* Es el conjunto de registros o datos referentes a una persona; (iv) *Recolección de la información:* Es la actividad consistente en el levantamiento físico o electrónico de la información, previa autorización del titular de la misma; (v) *Suministro de información.* Es la entrega de la información por parte de los operadores de los bancos de datos o centrales de información, autorizados por su titular; y (vi) *Titular de la información:* Toda persona natural o jurídica, pública o privada a quien se refiere la información y que repose en un banco de datos o centra de información.

El Hábeas Data era una Institución jurídica de naturaleza administrativa, pues el titular de los datos que le concernían podía recurrir dentro de los términos fijados en el 22 del proyecto, desde la fase de recolección hasta la fase de comunicación y suministro de datos en defensa de sus derechos fundamentales si éstos resultaren amenazados o vulnerados con el tratamiento informatizado o no, por los responsables de los bancos de datos o las centrales de información.

Así para la consultad de información, el titular de los datos disponía de 3 días hábiles para ser atendida su por los responsables de los bancos o las centrales de información. Para la actualización y la rectificación de los datos, según fuere el caso se disponía de 5 días hábiles para cada actividad. Si se desconocían los términos o se negare la petición respectiva, el titular de los datos podía interponer el recurso de reposición ante el operador del Banco de datos o la central de información. La apelación se podía interponer ante el Organismo de Control, que lo era la Superintendencia de Industria y Comercio, y en su nombre quien realice las funciones de protección al consumidor. Se aplicaba las normas del C.C.A. (Código Contencioso Administrativo de 1984-89, hoy derogado por el C.P.A. y C.A), para los efectos de los recursos administrativos, forma y efectos jurídicos.

2.3.3. El Proyecto de Ley Estatutaria No. 201 de 2003: Hábeas Data de carácter administrativo de conocimiento de la Defensoría del Pueblo, aplicado a los datos personales con énfasis en el dato financiero

El proyecto de 2003 tenía por objeto “desarrollar el derecho a acceder a la información de interés público, en particular la de carácter comercial y financiera, así como aquella relacionada con el cumplimiento e incumplimiento de las obligaciones fiscales, parafiscales, de servicios públicos domiciliarios, recolectada en bancos de datos o centrales de información. Para tal fin, se regula el ejercicio de la actividad de recolección, almacenamiento, procesamiento, suministro y uso de tal información”.

Sin incluir el término, Hábeas Data en el intitulado del proyecto de ley dentro del amplio catálogo de definiciones técnico-jurídicas incluye una definición cerrada de Hábeas Data, así: “Derecho fundamental autónomo que confiere a su titular las facultades de conocer, acceder, actualizar, rectificar y en general, controlar, los datos e informaciones que se hayan recogido sobre las personas en bancos de datos y en archivos de entidades públicas y privadas”.

Por su parte, en otra de las definiciones que complementa el entendimiento de Hábeas Data, manifiesta que “procesamiento o tratamiento de información, es cualquier operación o conjunto de operaciones y procedimientos, de carácter automatizado o no, que permitan la recolección, registro, grabación, organización, conservación, elaboración, modificación, circulación, bloqueo y cancelación de datos así como las cesiones de comunicaciones, consultas, interconexiones y transferencias”.

De las dos definiciones se conceptualiza que el Hábeas Data es un mecanismo jurídico que puede ser utilizado por la persona concernida con los datos para solicitar ante los responsables de los bancos de datos o las centrales de información, la aprehensión del conocimiento, acceso y llegado el momento y eventualidades, la actualización, rectificación y eliminación de los datos personales, siempre que se hayan recabado o tratado con medios informatizados o no, sean éstos públicos o privados.

Sin embargo esta conceptualización se complementa con una serie de principios aplicables a las fases del tratamiento de datos en general como en especial a los aplicables a la propia institución del Hábeas Data. En efecto, el proyecto al redirigir uno de los principios del tratamiento de los datos al Hábeas Data, le brinda un plus de protección y defensa a los titulares de los datos y a la vez, al conectarlo el llamado derecho de la “Libertad informática” de que hablara la jurisprudencia del Tribunal Constitucional de España en la Sentencia STC 254 de 1993, parecería estar blindando exageradamente el derecho de Hábeas Data.

El mencionado principio sostenía: “Del Habeas Data y la libertad informática”. Este principio consistía en que “todas las personas 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”. Y agregaba en los incisos 2º y 3º: “En la recolección, tratamiento y circulación de datos se deben respetar la libertad y demás garantías consagradas en la Constitución. Los datos personales deberán ser recogidos y tratados mediante la más escrupulosa observancia de las normas vigentes y el respeto de la dignidad de sus titulares.

El Proyecto estructuró además un procedimiento breve y sumario de Hábeas Data de carácter administrativo el cual conocía la Defensoría del Pueblo, como organismo de vigilancia y control de la protección de los datos personales en Colombia.

2.3.4. El Proyecto de Ley Estatutaria No. 64 de 2003 acumulado al Proyecto No. 074 de 2003: El Hábeas Data de carácter administrativo mediante el “procedimiento de amparo informático” y de conocimiento de la Defensoría del Pueblo y/o el Habeas Data jurisdiccional originado por la acción de tutela, aplicado en forma integral a los datos personales

La defensoría del Pueblo en Colombia, presentó en el año de 2003, el proyecto de Ley Estatutaria del Hábeas Data No. 064, *“Por el cual se dictan disposiciones para la protección de datos personales y se regula la actividad de recolección, tratamiento y circulación de los mismos”*, el cual fue acumulado al Proyecto No.074 de 2003 de la Cámara de Representantes, *“por la cual se regula integralmente el derecho fundamental al hábeas data y demás libertades y derechos fundamentales de las personas en lo que respecta al tratamiento de sus datos personales a través de bases de datos públicas y privadas, y se dictan otras disposiciones”*, los cuales no se convirtieron en ley de la República por falta de trámite.

Desde el mismo objeto e intitulado del proyecto No. 064 de 2003, se hallan elementos definidores de la conceptualiza el Hábeas Data, pues el artículo 1º al propende por el desarrollo del *“derecho fundamental de hábeas data para la protección de datos personales y para garantizar que en la recolección, tratamiento y circulación de tales datos se respeten la libertad, la honra, la intimidad personal y familiar y demás derechos fundamentales de todas las personas en Colombia”*, establece de forma inequívoca que la institución jurídica del Hábeas Data, puede comenzarse a construir con dos de los elementos esenciales inmersos en el intitulado y objeto proyecto, a saber: (i) La protección de las fases del tratamiento de los datos; y, (ii) la institucionalización de garantía legal para otros derechos.

Los restantes elementos definidores se hallan relacionados en los artículos 12 y 13 del proyecto y más específicamente en Capítulo II dedicado al “Derecho de Habeas Data”, en el que se describen a partir del artículo 14, el alcance, rectificación, notificación a terceros, actualización, supresión, eficacia de la supresión, bloqueo y la impugnación de las decisiones automatizadas y ejercicio de los derechos, legitimidad; entre otros.

Para abundar sobre la conceptualización el artículo 5-3 del proyecto de Ley estatutaria, suministraba una definición cerrada de Hábeas Data en los siguientes términos:

El Hábeas Data, es un derecho fundamental autónomo que confiere a su titular las facultades de solicitar y obtener la actualización, rectificación, bloqueo y supresión de la información que le concierne, recogida o registrada en bancos de datos o archivos de entidades públicas o privadas y, en general, mantener el control de los datos de los que es titular para que su tratamiento, uso o divulgación se haga con pleno respeto a los derechos y garantías constitucionales y legales.

A tenor del artículo 79 del proyecto de ley, “el procedimiento de amparo informático” (que hasta ese momento no tenía antecedente sin par en los proyectos de leyes sobre Hábeas Data en Colombia), sostenía que el *“ejercicio del derecho de acceso o del derecho de Hábeas Data, cualquier persona podrá presentar una solicitud de amparo informático ante la Defensoría del Pueblo, cuando quiera que estime que sus derechos fundamentales han sido desconocidos, afectados o amenazados en relación con el tratamiento a que han sido sometidos sus datos personales o información que le concierna directamente”*

Para que sea viable este procedimiento administrativo que generaba el Hábeas Data, se exigía el cumplimiento de un presupuesto previo de admisibilidad. En efecto, el artículo

80, manifestaba que era *“necesario que el interesado, en ejercicio de sus derechos de acceso o hábeas data, presente su solicitud de acceso, rectificación, actualización, bloqueo o supresión de datos de manera previa ante la fuente de información o banco de datos responsable del tratamiento”*. Y agregaba el inciso 2º, *“En caso de que la respuesta sea desfavorable, no resulte satisfactoria o no haya pronunciamiento para el titular de los datos, éste quedará habilitado para recurrir ante la Defensoría del Pueblo, para la efectividad de sus derechos fundamentales”*.

Finalmente, el proyecto de ley proporcionaba al titular de los datos para escoger a voluntad entre el trámite y procedimiento originado por el Hábeas Data en el ámbito administrativo ante la defensoría del Pueblo, o el trámite y procedimiento originado en la acción de tutela en el ámbito jurisdiccional ante la justicia constitucional (jueces, tribunales y Altas Cortes) que en nuestro criterio creaba una especie de Hábeas Data de carácter jurisdiccional.

El artículo 84 del proyecto establecía una regla especial y de prevalencia sobre la escogencia del Hábeas Data administrativo o jurisdiccional, al sostener que: *“la acción de tutela excluye el amparo informático. Se entenderá que por la presentación de la solicitud, el titular de los datos declara bajo la gravedad del juramento que no ha iniciado ni se encuentra en curso ni existe fallo proferido en acción de tutela interpuesta por los mismos hechos y derechos que reclama en ejercicio del amparo informático”*.

2.3.5. El Proyecto de Ley Estatutaria de Hábeas Data de 2005: El Habeas Data administrativo (defensoría del Pueblo) y Habeas Data jurisdiccional (justicia constitucional), aplicado en forma integral a los datos personales

El proyecto de 2005, *“Por el cual se dictan disposiciones para la protección de datos de carácter personal y se regula la actividad de recolección, tratamiento y circulación de los mismos”*, contenía los lineamientos, estructura y contenidos programáticos y normativos de los proyectos de ley presentados a instancia de la Defensoría del Pueblo en los años 2003 y 2004, pero reestructurados tanto en sus títulos, capítulos y artículos de forma tal que presentaban no solo un texto depurado sobre el Hábeas Data sino conciliado con nuevas y actualizadas técnicas jurídicas, con definiciones y principios más acordes con el tratamiento de datos y la mejor presentación del Hábeas Data administrativo y jurisdiccional.

En el artículo 5º numerales 3º y 4º se suministran definiciones cerradas del Hábeas Data en general y el Habeas Data colectivo, así: El Hábeas Data, en general es el *“derecho fundamental autónomo que confiere a su titular, sus representantes o causahabientes, las facultades de solicitar y obtener del banco de datos información acerca de la existencia o no de un tratamiento de datos que le conciernen, los fines y la forma como se lleva a cabo dicho tratamiento, la clase de datos objeto de tratamiento, los destinatarios o clase de destinatarios a quienes se han suministrado los datos, y la fuente u origen de ellos; de solicitar la actualización, rectificación, disociación y supresión de la información de la cual es titular en los casos que contempla la ley y, en general, de mantener el control sobre ella para que su tratamiento, uso o divulgación se haga con pleno respeto a los derechos y garantías constitucionales y legales”*.

El Hábeas Data Colectivo, *“es un derecho que permite a cualquier persona, organización o al Defensor del Pueblo, solicitar la suspensión, rectificación o cesación de un tratamiento de datos que se está realizando de manera irregular, con pretermisión de los requisitos establecidos para ello, o respecto de datos que no pueden ser objeto de*

tratamiento o cuyo tratamiento está sujeto a condiciones o requisitos que no se han cumplido y que afecta a una generalidad o grupo de personas determinadas o no”.

Se ratifica la existencia y trámite del procedimiento de amparo informático de carácter administrativo ante la Defensoría del Pueblo y Registro Nacional Público de Bancos de Datos y el procedimiento jurisdiccional originado en la acción de tutela para efectivizar el Hábeas Data ante la justicia constitucional colombiana, a libre escogencia del titular de los datos personales tratados, procesados y recabados en bancos de datos o centrales de información de ámbito público y privado y cuando se halle en las eventualidades de amenaza o vulneración de los derechos fundamentales contemplados en la Constitución de 1991, pero principalmente del derecho de la intimidad, el honor y el buen nombre.

2.3.6. La Ley 1266 de Diciembre 31 de 2008: El Hábeas Data administrativo (Superintendencia de Industria y Comercio y Financiera, según la materia tratada) y el Hábeas Data jurisdiccional (acción de tutela), aplicado enfáticamente al dato financiero

La Ley 1266 de 2008, recogió en su integridad lo previsto en los proyectos de Ley Estatutaria número 221/2007 de la Cámara de Representantes y el número 027/2006 del Senado de la República, acumulados con el proyecto de Ley Estatutaria de Hábeas Data número 05/2006 Senado, *“Por el cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial y de servicios y se dictan otras disposiciones”*, que finalmente se convertiría en la Ley de Habeas Data Financiero de Colombia.

La Ley Estatutaria de 2008 es una Ley que pretende ser general y no integral sobre el Hábeas Data y el derecho de acceso a la información de naturaleza con énfasis en la información financiera ^[48] de carácter privado y también pública.

Como en los proyectos de Ley, en el intitulado y el objeto de la Ley 1266 de 2008, se hallan elementos definidores de la conceptualización del Hábeas Data. En efecto, en el artículo 1º, al describir el objetivo de la ley manifiesta: *“desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos, y los demás derechos, libertades y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales a que se refiere el artículo 15 de la Constitución Política, así como el derecho a la información establecido en el artículo 20 de la Constitución Política, particularmente en relación con la información financiera y crediticia, comercial y de servicios”*.

De lo cual se deduce que la institución del Hábeas Data en Colombia persiste en la regulación marcadamente sectorial que regula con demasiado énfasis el dato financiero: comercial, bancario y tarifario o de servicios públicos domiciliarios, pese a que pretende ser de carácter general. En la búsqueda de esa generalidad, el actual proyecto mejora el

(48) En diferentes proyectos de regulación del Hábeas Data en Colombia, bien de iniciativa gubernamental o parlamentaria durante estos 16 años de no reglamentación de la Constitución sobre el particular, se ha observado que proyectos con trabajo intelectual propio de los juristas colombianos, que son muy pocos; y otros, que han solicitado en préstamo dicho labor y han preferido seguir modelos latinoamericanos. El presente proyecto con énfasis en el dato financiero sigue muy de cerca de la ley No. 17938 de Octubre 1º de 2004 o *“Ley de protección de datos personales para ser utilizados en informes comerciales y el Hábeas Data”* del Uruguay (LPDP_HDU), y en lo pertinente al dato financiero a la Ley de Protección de Datos personales Argentina de 2000.

contenido, aunque presenta una estructura normativa cuestionable frente a los anteriores presentados al Congreso de la República, tanto los de iniciativa gubernamental (Ministerio de Hacienda Pública y crédito público) como los de iniciativa parlamentaria e incluso los de iniciativa acumulada.

Algunos de esos elementos definidores de la conceptualización del Hábeas Data son: (i) Es un derecho fundamental de toda persona tendiente a conocer, actualizar y rectificar las informaciones recabadas en bancos de datos informatizados o no; (ii) Los datos personales están sometidos a unas fases del tratamiento de datos, tales como la recolección, “tratamiento” propiamente dicho y la circulación (o mejor comunicación); (iii) Constituye una garantía constitucional de otros derechos (ya no solo de la intimidad, el honor y el buen nombre), “libertades y garantías constitucionales”. Si el Hábeas data por definición es una garantía constitucional, al garantizar otras garantías constitucionales como pretende la Ley, aquél se convertirá en una garantía plus de los derechos constitucionales; y, (iv) el derecho a la información aún siendo autónomo e independiente del Hábeas Data, en el presente proyecto se desarrolla parcialmente, a efectos de servir de fundamento no solo para la conceptualización del Hábeas Data sino como parte sustancial de éste.

Completan los elementos definidores de la conceptualización del Hábeas Data algunas definiciones relacionadas en la ley en el artículo 3º, pero principalmente las referidas a los datos personales, al dato público, el dato privado y el dato “semi-privado”. Sobre éste último manifiesta la ley, aplicándolo casi en forma exclusiva y excluyente al dato financiero que éste es *“el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios...”*^[49].

Por si fuera poco, la ley de Hábeas Data con énfasis en el dato financiero, incluye una definición técnico-jurídica cerrada aplicable al tratamiento de datos personales. Esta se refiere a la *“Información financiera, crediticia, comercial, de servicios y la proveniente de terceros países”*, la cual se entenderá como la *“información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, aquella referida al nacimiento, ejecución y extinción de obligaciones dinerarias, independientemente de la naturaleza del contrato que les dé origen, así como la información relativa a las demás actividades propias del sector financiero o sobre el manejo financiero o los estados financieros del titular”* (artículo 3º, literal j), de la Ley citada).

Toda clase de información proveniente de “terceros países” obedece al fenómeno de los medios TIC que hoy son la forma normal y corriente de comunicar datos de todo tipo y no solo los financieros. Por ello resulta casi impertinente individualizar una fase del tratamiento de datos como es la comunicación o circulación de datos (que los europeos

(49) Esta categorización de los datos personales en el proyecto de Hábeas Data colombiano era puesta en la escena doctrinal con cierto halo de desjudicialización o de exclusión de control administrativo, por parte del Presidente de Computec S.A., al sostener que “La naturaleza del Hábeas Data de tipo crediticio es diferente a otras manifestaciones del mismo derecho, como el hábeas data de información pública o de información sensible. En efecto en Colombia, así como ha ocurrido en otras latitudes, el dato personal de tipo crediticio es considerado como un dato, que aunque privado, no está en la esfera íntima de las personas, razón por la cual es permitida su circulación cuando preexista una autorización del titular para ello, o inclusive –como ocurre en algunos países– cuando quien suministra el dato es un acreedor del reportado o alguien con un interés jurídico legítimo para reportarlo”. Cfr. VILLAVECES HOLLMANN, Juan Manuel. **Reflexiones en torno a la necesidad de un marco regulatorio sobre Hábeas Data**. En: Foro Universidad de los Andes, Noviembre 18 de 2003.

prefieren denominar: “flujo o movimiento internacional de datos”) para el dato financiero cuando es una característica general de todo dato o información sea o no personal, privada o pública.

2.4. El Hábeas Data en la doctrina nacional y extranjera

Son tantas las definiciones como los autores que las suministran y por ello conviene analizarlas más desde el punto de vista de la naturaleza jurídica (como derecho, recurso, acción, garantía, “procedimiento” o institución jurídica de derecho público) en la que los tratadistas del derecho público encasillan al Hábeas Data, que en la mera relación de las mismas según la nacionalidad de los autores. Esto nos permite adicionalmente derivar algunas de las características más relevantes del Hábeas Data, como la autonomía, la de ser un derecho de aplicación inmediata, un derecho de tercera “generación” productos de las nuevas tecnologías de la información o la comunicación (TIC) y la informática; entre otras.

2.4.1. El Hábeas data como derecho fundamental

Esta corriente del pensamiento jurídico Latinoamericano se consolida en el derecho público colombiano, tras el advenimiento y la clasificación de los derechos constitucionales de las personas previstos en la Constitución Política de 1991. En efecto, los derechos a tenor del Título II, “*De los derechos, garantías y deberes*” se clasifican así: (i) Capítulo Primero: “*Derechos Fundamentales*” artículos 11 a 41. El artículo 15 incisos 1º y 2º y el artículo 20 regulan el Hábeas Data y el derecho a la información respectivamente. Este último aplicable al Hábeas Data, tan solo en la arista de informar y ser informado sobre sus datos o informaciones personales o familiares y ejercer su control^[50]; (ii) Capítulo Segundo: “*Derechos Sociales, económicos y culturales*” artículos 42 a 77. El artículo 74 relativo al derecho de acceso a la información pública, pese a estar ubicado en el título segundo, es un derecho fundamental que incide en la órbita personal del ser humano y por tanto en el Hábeas Data, que *ab initio* es un derecho de la protección de los datos o informaciones de la persona; y, (iii) Capítulo Tercero: “*Derechos Colectivos y del ambiente*” artículos 78 a 82.

Por eso, el jurista *Cifuentes Muñoz* ^[51] ha sostenido al respecto que “no se ha puesto jamás en duda que el Hábeas Data ostente la condición de derecho fundamental”, pues éste como derecho subjetivo vincula un elemento de la esencia de aquellos, cual es la dignidad del ser humano, que no solo es un principio constitucional (artículo 1º constitucional), sino un valor constitucional: fundamento y esencia del ordenamiento jurídico vigente y razón para la existencia de los derechos, deberes y garantías de la persona humana.

El Hábeas Data, atendiendo al criterio principal de la “dignidad de la persona humana” extractado por la jurisprudencia de la Corte Constitucional Colombiana, tal como lo expo-

(50) El Habeas Data confiere a la persona mecanismos para que controle el uso de su información personal y, al mismo tiempo, impone obligaciones a los administradores de archivos o bancos de datos para que no amenacen o vulneren los derechos fundamentales de las personas mediante el uso indebido de sus datos personales o de su plataforma tecnológica. REMOLINA ANGARITA, Nelson. *Del actual proyecto (No. 071 de 2002) de Ley estatutaria del Hábeas Data en Colombia*. Facultad de Derecho de la Universidad de los Andes. nremolin@uniandes.edu.co

(51) CIFUENTES MUÑOZ, Eduardo. *El Hábeas Data en Colombia*. Revista *Ius et Praxis*, Año 3, Número 1º, Facultad de ciencias jurídicas y sociales, Universidad de Talca, Talca (Chile), 1997 p.81-106

nen Gordillo y Restrepo ^[52] “constituye un derecho fundamental, en tanto garantía especial de la intimidad e integridad moral humana, pues le permite al hombre autodeterminarse en cuanto a la información que sobre la misma manejen otras personas o entidades, ora particulares, ora públicas; ‘...tanto el habeas data como la intimidad encuentran su razón de ser y su fundamento último en el ámbito de autodeterminación y libertad que el ordenamiento jurídico reconoce al sujeto como condición indispensable para el libre desarrollo de su personalidad y en homenaje justiciero a su dignidad (Sentencia T-022-1993)”

Se comprueba también que el Hábeas Data es un derecho fundamental porque es un derecho de aplicación inmediata, según el enlistamiento *numerus clausus* que realiza el artículo 85 de la Constitución de 1991, pues “no requieren de previo desarrollo legislativo o de algún tipo de reglamentación legal o administrativa para su eficacia directa y que no contemplan condiciones para su ejercicio en el tiempo, de modo que son exigibles en forma directa e inmediata (Sentencia T-002-1993)” ^[53].

Finalmente como derecho fundamental, el Hábeas Data también es de carácter subjetivo, pues es “invocable por sus titulares para tener conocimiento de los datos que las autoridades y los particulares hayan recogido sobre ellos y para introducir en las informaciones erróneas o desactualizadas las oportunas enmiendas... El derecho de habeas data nos otorga la posibilidad de percibir y controlar el empleo que otros hacen de nuestros antecedentes personales, con el fin de impedir que éstos se utilicen con fines censurables” ^[54].

2.5.2. El Hábeas Data es una acción jurisdiccional de amparo o tutela específico

En la mayoría de Estados Latinoamericanos el Hábeas Data desde su visión adjetiva o procedimental, se considera como una acción procesal de rango constitucional y con titularidad para toda persona, tanto si se denomina acción de amparo genérico o bien acción de amparo específico, pero en ambos casos con unas finalidades y propósitos predefinidos en los textos constitucionales y legales, dirigidos a proteger los datos o informaciones de las personas a quienes les concierne aquellos y se encuentren recabados en bancos de datos informatizados o no, como también a la defensa de los derechos y libertades constitucionales que pudieren verse amenazados o vulnerados con el tratamiento de datos indebido, ilegítimo o contrario al ordenamiento jurídico vigente.

Así lo confirman Baigorri, Juárez y López ^[55], en el ámbito argentino “gran parte de la doctrina y jurisprudencia consideran que el habeas data es una especie de amparo. Es decir, el amparo sería el género (art. 43 CN, 1° Párr.), que incluye diversas especies, entre ellas el habeas data. Es una variable de la acción de amparo (según Quiroga Lavié). Como ha dicho Sagües, ‘es una subespecie de amparo o amparo específico’”.

(52) GORDILLO T. José F. y RESTREPO, Yepes. **Introducción al análisis del derecho fundamental del habeas data**. En: <http://www.urosario.edu.co>

(53) Sentencia de la Corte Constitucional Colombiana, citada en la Ob., ut supra cit.

(54) Madrid-Malo Garizábal, Mario. **Derechos fundamentales**, 2 edición, Bogotá, Ed. Temas Jurídicos-3R Editores, 1997, p. 207. Citado por GORDILLO T. José F. et all.

(55) Quiroga Lavié, Humberto. **El amparo, el habeas data y el habeas corpus en la reforma de la constitución – Explicada por miembros de la comisión de redacción**. Rubinzal Culzoni. Santa Fe. 1994. p. 157, y Sagües, Néstor Pedro. **Amparo, habeas data y habeas corpus en la reforma constitucional**. En LL 1994-D-1157. Citados por BAIGORRI, Mauricio J., JUAREZ F. Martín., LOPEZ A., María J. **La naturaleza jurídica del Hábeas Data**. VIII Jornadas Argentinas de Derecho procesal constitucional. Estudiantes de la Facultad de Derecho y ciencias Sociales de la Universidad de Córdoba (Argentina). En: <http://www.salvador.edu.ar/>

En igual sentido se manifiesta Dubie^[56] “La subespecie de amparo que es el habeas data es un remedio muy específico y preciso que debe ser utilizado en situaciones extremas y delicadas y cuando no existan otros caminos aptos para resguardar la tutela de los derechos fundamentales; debiendo, quienes la incoa, acreditar haber realizado las gestiones o tramitaciones necesarias para acceder a los registros u obtener la información o rectificación requerida, o bien la inutilidad de los trámites administrativos... Por ende, la acción deducida se aprecia cuanto menos prematura y fue adecuadamente rechazada.”

Más aún, el “Hábeas Data es un subtipo de la acción de amparo o protección en cuanto ámbito del derecho procesal constitucional protector de derechos fundamentales o jurisdicción constitucional de la libertad, según la conocida expresión de Cappelletti y Fix Zamudio. Este es un derecho que le asiste a toda persona a solicitar administrativamente y judicialmente la exhibición de registros o bases de datos –públicos o privados—en los cuales estén incluidos sus datos personales o de su familia, para tomar conocimiento de su exactitud, solicitar su rectificación, superación (mejor, supresión), complementarlos o solicitar su reserva”^[57].

Debe aclararse que si bien el autor hace relación al Hábeas Data administrativo, como lo hemos llamado al desatado en vía administrativa con el objeto de petitionar, reclamar o recurrir por el acceso, conocimiento, actualización, rectificación y eliminación de los datos personales que le conciernen a una persona frente a bancos de datos públicos, la inclusión de la definición en este grupo donde se comenta el Hábeas Data jurisdiccional, es válida en el sentido de considerar al Hábeas data como una acción de amparo específico, independientemente de si es de carácter jurisdiccional o administrativo. La regla general, es que el Hábeas Data que se ejercita en los Estados Latinoamericanos es de índole jurisdiccional y por excepción de ámbito administrativo. Circunstancia diferente es que en algunas legislaciones de Latino América, se exija el agotamiento de una vía previa administrativa antes de acudir a la vía jurisdiccional de Hábeas Data.

Para Palazzi^[58], “El hábeas data puede ser concebido como una acción judicial (de amparo) para acceder a registros o bancos de datos, conocer los datos almacenados y en caso de existir falsedad o discriminación corregir dicha información o pedir su confidencialidad”. Con lo cual no reconoce la existencia del Hábeas data de carácter administrativo o no jurisdiccional que bien puede presentarse en el derecho argentino como el colombiano.

Tan sólo en el ámbito del derecho público colombiano, existe la acción de tutela específica del Hábeas Data, con esa denominación, pues hoy para hacer efectivo el núcleo esencial del Hábeas Data previsto en el artículo 15 Inciso 1º y 2º de la Constitución de 1991, y consistente en el uso y control de los datos personales que a la persona le conciernen y en el libre y potencial ejercicio de reacción ante quienes abusen o los utilicen indebida, ilegítima o contrariamente al derecho; la acción de tutela genérica tal como está prevista en el artículo 86, constitucional y el Decreto reglamentario 2591 de 1995, es el mecanismo constitucional de carácter jurisdiccional idóneo ante la justicia constitucional

(56) DUBIE, Pedro. **El Hábeas Data financiero**. Revista de Derecho Informático. ISS 1681-5726. Ed. Alfa-Redi, No. 038, Septiembre de 2001

(57) NOGUERA ALCALA, Humberto. **Reflexiones sobre el establecimiento constitucional del Hábeas Data y del proyecto en tramitación parlamentaria sobre la materia**. Revista Ius et Praxis, Número 1º, Facultad de ciencias jurídicas. Universidad de Talca, Talca (Chile), 1997, p. 265-284

(58) PALAZZI, Pablo. **El Hábeas Data en el derecho Argentino**. Revista de Derecho Informático. ISSN 1681-5726, Edita: Alfa-Redi No. 004 - Noviembre del 1998. En: <http://www.alfa-redi.org>

(jueces, autoridades judiciales, tribunales y Altas Cortes), no solo para proteger y garantizar el derecho fundamental de Hábeas Data sino los demás derechos fundamentales previstos en el Título II de la Constitución y aquellos que sin estar en éste título se consideran como tales (v.gr. el derecho de acceso a la información pública, estipulado en el artículo 74).

En tanto, no exista legislación integral y específica que desarrolle los artículos correspondientes a la estructuración del Hábeas Data en Colombia, la acción de tutela es el mecanismo jurisdiccional para hacer efectivo esas "*varias facultades de la persona concernida por los datos*" ^[59] (estimamos se refiere el autor al acceso, conocimiento, actualización, rectificación y eliminación) y previstas principalmente en los incisos 1º y 2º del artículo 15. Incluso aun existiendo la norma legal, tal como se perfila con el proyecto de ley estatutaria de 2007 que reglamenta sectorialmente el Hábeas Data, el mecanismo idóneo seguirá siendo la acción de tutela en sede jurisdiccional, pues el proyecto así lo prevé, junto a la existencia del Hábeas Data en sede administrativo ante los organismos de control o ante las personas públicas o privadas responsables de los bancos de datos o "centrales de información financiera".

2.5.3. La acción de Hábeas Data es una garantía o "remedio" ^[60] constitucional

En este aparte entendida la garantía constitucional, como lo explicaba el tratadista latinoamericano Héctor Fix Zamudio ^[61], es decir, que las garantías son "*instrumentos procesales aptos para la defensa de los derechos fundamentales*".

La Constitución peruana expresamente en el artículo 20, intitula: "*Garantías constitucionales*" y en el contenido de la norma se refiere a las acciones de Hábeas Data, Hábeas Corpus, de inconstitucionalidad, la de amparo, etc., De lo cual se infiere que las acciones inmersas en ese intitulado bien pueden denominarse: "acciones de garantía". Quizá por ello, denominar al Hábeas Data como garantía no es un pleonismo jurídico sino una realidad normativa de índole constitucional en aquél país, y por eso se afirma que "*La Acción de Hábeas Data es una garantía constitucional, de naturaleza procesal sumaria, que procede contra el hecho u omisión, por parte de cualquier autoridad, funcionario o persona, que vulnera o amenaza derechos constitucionales informáticos*

(59) El Autor considera que la respuesta del derecho frente a las nuevas tecnologías TIC y la informática, "no se endereza a suprimir este nuevo factor de control social. El Hábeas Data representa apenas un intento incipiente y tímido, dirigido a corregir distorsiones extremas del proceso comunicativo informático. De un lado, reduce en cierto grado la invisibilidad de los gestores o titulares de los bancos de datos –lo que se logra exigiendo un registro de bancos, una declaración de sus objetivos y de sus procedimientos, etc.–, de otro lado, permite a las personas, en cierta medida, adquirir consciencia de su transparencia externa y de las condiciones de la misma, pudiendo incidir en la elaboración y transmisión de formatos singulares o unidimensionales de su personalidad y de sus acciones. La diferenciación entre información sensible o no sensible, resulta esencial para determinar la extensión y los límites de los poderes informáticos" CIFUENTES MUÑOZ, Eduardo. *El Hábeas Data en Colombia...* Ob., ut supra cit.

(60) En opinión de Alfonso Da Silva, el hábeas data (art. 5º; LXXII) es un remedio constitucional, un medio destinado a provocar la actividad jurisdiccional y que, por tal motivo, tiene naturaleza de acción, más específicamente de acción constitucional. A su vez, cobija un derecho –el derecho de conocimiento de datos personales y de rectificarlos–, que en vez de ser reconocido de forma independiente, está contenido en la garantía que lo ampara. Vid. DA SILVA, José Alfonso. *Curso de direito constitucional positivo*, p. 386 y 397. Citado por PUCCINELLI, Oscar *El Hábeas Data en el Brasil*. En: www.astrea.com.ar

(61) GARCIA BELAUNDE, Domingo. *Diferencias entre el Hábeas Data y la acción de amparo o tutela constitucional en Perú*. Revista Ius et Praxis, Año 3, Número 1º, Facultad de ciencias jurídicas y sociales, Universidad de Talca, Talca (Chile) 1997, p. 179-188

considerados en los numerales 5) y 6) del Artículo 2º de la Carta Magna”^[62], es decir, de una parte, el derecho a solicitar y recibir información de una entidad pública, excepto las referidas a la intimidad personal, la referidas a la seguridad nacional y las que estén previstas en la ley; y de otra, los derechos referidos a los “servicios informáticos, computarizados o no, públicos o privados, (y que) no suministren informaciones que afecten la intimidad personal y familiar”.

En el derecho público ecuatoriano la acción de Hábeas Data, también se considera una garantía constitucional, ya que “tiene estrecha relación con los derechos de las personas protegidos por los números 8 y 21 del artículo 23 de la misma, a saber: El derecho a la honra y a la buena reputación y a la intimidad personal y familiar”; y, “El derecho a guardar reserva sobre sus convicciones políticas y religiosas. Nadie podrá ser obligado a declarar sobre ellas. En ningún caso se podrá utilizar información personal de terceros sobre sus creencias religiosas y filiación política, ni sobre datos referentes a salud y vida sexual, salvo para satisfacer necesidades de atención médica”. Este segundo derecho protegido por nuestra Norma Suprema, tiene también relación con el derecho a la intimidad señalado por el primero de los numerales anotados”^[63]. Pero también como lo denota la Comisión Andina de Juristas^[64], el Tribunal Constitucional del Ecuador en algunos pronunciamientos ha sostenido el Hábeas Data es una “garantía constitucional, (que) protege “el derecho que tienen las personas naturales y jurídicas a acceder a los documentos, bases de datos e informes que sobre sí mismas o sus bienes, se encuentran en poder de entidades públicas o privadas, inclusive de personas naturales o jurídicas privadas y conocer el uso que se esté dando, que se dio o que se va a dar a tal información y, por ende obtener acceso directo, cabal y verídico de ella, así como a que se rectifiquen, se eliminen o no se divulgue, según el caso los datos que el recurrido posea” (Sentencia del 22 de septiembre de 1999)

En el ámbito venezolano, la Constitución de 1999 consagra en el artículo 28 la institución jurídica del Hábeas Data, no expresamente en el *nomen iuris* sino en el contenido de las facultades inherentes a la institución y derecho de toda persona concernida, tales como conocer, acceder, rectificar, actualizar y/o solicitar la eliminación de información personal errónea, ilegítima o no conforme al derecho que se haya recabado en registros de datos públicos o privados. Sin embargo, la Exposición de Motivos de la Constitución sí se hace mención expresa del Hábeas Data, cuando se manifiesta que “se reconoce por vez primera en el constitucionalismo venezolano, el hábeas data o derecho de las personas de acceso a la información que sobre sí mismas o sobre sus bienes consten en registros oficiales o privados...(éste) incluye el derecho de las personas a conocer el uso que se haga de tales registros y su finalidad, y de solicitar ante tribunal competente su actualización, rectificación o destrucción, si fuesen erróneos o afectasen ilegítimamente sus derechos”.

El Hábeas Data en Venezuela además de ser una garantía constitucional es también un derecho fundamental no solo por su ubicación y clasificación en el texto constitucional del 99 sino por ser de aplicación inmediata y estar fundado en el valor de la dignidad humana. Como garantía se ha sostenido que “La acción se define como el derecho que asiste a

(62) NUÑEZ PONCE, Julio. **La Acción Constitucional de Habeas Data y la Comercialización de Información Judicial en Internet**. Revista de Derecho Informático. ISSN 1681-5726, Edita: Alfa-Redi No. 013 - Agosto del 1999. En: <http://www.alfa-redi.org>

(63) GARCIA BERNI, Aida. **La acción de Hábeas Data**. Asesora del Tribunal Constitucional Ecuatoriano. En: <http://www.dlh.lahora.com.ec>

(64) AA.VV. **El proceso de Hábeas data en la Región Andina**. En: www.cajpe.org.pe/

toda persona (identificada o identificable) a solicitar judicialmente la exhibición de los registros (públicos o privados) en los cuales están incluidos sus datos personales o los de su grupo familiar, para tomar conocimiento de su exactitud; a requerir la rectificación, la supresión de datos inexactos u obsoletos o que impliquen discriminación . . . Tiende a proteger a la persona contra calificaciones sospechosas incluidas en registros que pueden llegar a perjudicarlo de cualquier modo" [65].

En el ámbito del derecho argentino, un sector de la doctrina que considera el Hábeas data como una "variable del derecho a la intimidad", reconoce "como novedad absoluta dentro de las garantías constitucionales introducidas por la reforma se encuentra el "hábeas data" o derecho de toda persona a interponer la acción de amparo "para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en tal caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos " [66].

Pero otro sector de la doctrina argentina, sostiene que "la garantía constitucional del hábeas data es un importantísimo desarrollo jurídico- institucional que, como todo en estos complejos ámbitos, perfecciona el ejercicio de un aspecto e impactan sobre otros limitándolos, concretamente sobre la libertad de expresión- derecho a la información, a la comunicación" [67]. Obviamente que la autora estudia y analiza las tensiones (o "conflictos") y posibles soluciones que se presentan entre derechos de igual rango constitucional, como lo son la "garantía del derecho a la intimidad" y la garantía del Hábeas Data para llegar a establecer el impacto jurídico de una y otra garantía frente a los derechos de información y comunicación y la libertad de expresión. En este contexto se debe entender su definición.

2.5.4. El Hábeas Data como proceso constitucional

García Belaunde [68] luego de una breve disquisición sobre el concepto jurídico de garantía como equivalente a derecho, garantía como acción procesal, termina diciendo que la garantía en el "concepto moderno y científico" es "proceso", pues "la acción es algo abstracto, que sirve para iniciar algo, pero la acción en sí misma no es nada. Entonces lo primero sería ponernos de acuerdo con el concepto...parte de la doctrina latinoamericana ya empieza a hablar de procesos constitucionales, a raíz de la Constitución del Brasil...(y)... han trabajado esos instrumentos como son el Hábeas Data, la Injunção, el mandato de segurança, etc."

En el derecho público peruano ha hecho carrera la expresión proceso o procedimiento cuando se van a referir al Hábeas Data y sobre todo a labor garantista que aquél ha desatado al denominarse así al Hábeas data. *Velezmoro* al respecto sostiene: "mas es desde el Habeas Data como proceso constitucional que protege el derecho de la persona sobre sus datos personales desde donde se ha logrado establecer la serie de facultades y poderes que caracterizan esta institución. Así, el recientemente promulgado...Código

(65) AA.VV. *La acción de hábeas data*. DDG-167-01/ 16-07-2001. En: <http://www.defensoria.gov.pe/>

(66) SANCHEZ, Mariana. *El Hábeas Data*. En: marianasanchez@fibertel.com.ar

(67) MARTELLA, Lilián P. *Hábeas Data: Garantía de una dimensión fundamental de la libertad*. UNRC-ICALA.

(68) GARCIA BELAUNDE, Domingo. *Diferencias entre el Hábeas Data...* Ob., ut supra cit.

Procesal Constitucional señala en su art. 61-1 que toda persona puede acudir a dicho proceso para: *conocer, actualizar, incluir, suprimir o rectificar la información o datos referidos a su persona que se encuentren almacenados o registrados en forma manual, mecánica o informática, en archivos, banco de datos o registros de entidades públicas o de instituciones privadas que brinden servicio o acceso a terceros. Asimismo, a hacer suprimir o impedir que se suministren datos o informaciones de carácter sensible o privado que afecten derechos constitucionales* ^[69].

En el derecho público argentino también existe un amplio sector de la doctrina que sostiene que el hábeas data más que un derecho fundamental es un proceso constitucional porque sirve *“herramienta procesal que la Constitución dispone para afianzar el cumplimiento de los derechos fundamentales”*, tales como la intimidad, el honor, la imagen, la reputación, la identidad, entre otros. Por eso, como sostiene Gozaini ^[70] *“a partir del derecho de amparo creado por la Constitución Nacional, se perfila este proceso constitucional específico de protección a la persona agredida o amenazada por los bancos de datos que aprovechan la información personal que le concierne”* denominado proceso constitucional de Hábeas Data.

En el ámbito ecuatoriano también se habla de proceso constitucional no solo en la doctrina calificada sino en los pronunciamientos del Tribunal Constitucional, tal como lo ejemplifica la Comisión Andina de juristas ^[71]. En efecto, “sobre el hábeas data, el Tribunal Constitucional del Ecuador ha precisado que el fin primordial de este proceso consiste en *“detener los abusos que puedan suceder con la manipulación de la información”* (Sentencia del 21 de enero de 1999), aunque reconocen que *“el proceso de hábeas data tiene una presencia discreta en el sistema constitucional del Ecuador. Así por ejemplo, la revisión de este proceso representa un porcentaje pequeño de los casos resueltos por el Tribunal Constitucional. En 1999, los hábeas data representaron solamente el 3.7% (35 casos) (Informe del Tribunal Constitucional del Ecuador al Congreso Nacional (enero-diciembre de 1999).*

2.5.5. El Hábeas Data como una acción exhibitoria de datos personales

Si bien toda acción de carácter jurisdiccional o administrativo tiene por objeto servir de instrumento procesal idóneo para iniciar un procedimiento, en el derecho brasileño y en el hondureño, cuando se refieren al Hábeas Data lo hacen recordando como dijimos en la etimología de la institución, el ancestro jurídico del derecho romano referido a los interdictos exhibitorios de personas, objetos, cosas, documentos y bienes muebles o inmuebles. Estos interdictos exhibitorios se han mantenido por siglos para las personas (Hábeas Corpus), pero muy recientemente se los ha aforado para la exhibición de documentos o datos personales sean sometidos o no a tratamiento informatizado por parte de la persona concernida con éstos, para lograr entre otras finalidades, controlar el

(69) El Código Procesal Constitucional, fue aprobado por Ley N° 28237, publicado el 31 de mayo de 2004. Dicha ley recoge el texto del Anteproyecto (salvo por el art. 63° referido a la ejecución anticipada de la sentencia que declara infundado el habeas data) presentado por un grupo de docentes universitarios en el 2003. Cfr. VELEZMORO PINTO, Fernando Rafael. **La tutela de la persona frente a los avances de la informática y la necesidad de avanzar más allá del derecho a la protección a los datos personales**. En: <http://www.latinoamericann.org/>

(70) “El habeas data no es un derecho fundamental stricto sensu –dice de Slavin-, sino que se trata de un proceso constitucional. Nos hallamos frente a un instrumento procesal destinado a garantizar la defensa de la libertad personal en la era informática”. Vid. GOZAINI, Osvaldo A. **El Proceso de Hábeas Data en la Nueva Ley (de protección de datos Argentina)**. Vía Internet.

(71) AA.VV. **El proceso de Hábeas data en la Región Andina**. En: www.cajpe.org.pe/

uso y utilización por terceras personas (responsables de los bancos de datos o “centrales de información” sectorial, como la financiera) de los datos de la persona (libertad informativa o libertad de control de los datos).

En el derecho brasileño, la acción exhibitoria de datos personales tiene por objeto *"asegurar el conocimiento de informaciones relativas a la persona del impetrante, que constan en los registros o bancos de datos de las entidades gubernamentales o de carácter público; rectificar datos, cuando no se prefiera hacerlo por proceso secreto, judicial o administrativo; y anotar, en las asientos correspondientes al interesado, la contestación o explicación justificable de un dato verdadero, y que estaba cuestionado judicial o amistosamente"* (Artículo 7)^[72].

En el derecho hondureño, el artículo 182 de la Constitución regula en forma conjunta las acciones o garantías constitucionales del Habeas Corpus, la cual la denomina “exhibición personal” y el Hábeas Data (o de exhibición de los datos personales). Esta última *“únicamente puede promoverla la persona cuyos datos personales o familiares consten en los archivos, registros públicos o privados”* para *“acceder a la información sobre sí misma o sus bienes en forma expedita y no onerosa, ya esté contenida en bases de datos, registros públicos o privados y, en caso de que fuere necesario, actualizarla, rectificarla y/o enmendarla”* y *“para hacer cesar cualquier violación a los derechos del honor, intimidad personal o familiar y la propia imagen”*.

En todo caso se debe aclarar que las acciones exhibitorias de Hábeas Data y Hábeas Corpus, en el constitucionalismo hondureño resultan meramente nominales, pues la acción constitucional que efectivamente posibilita la exhibición de los datos de la persona o de sus bienes o de la exhibición de la persona, según fuere el caso y acción respectiva, es la acción de amparo, como *“instrumento jurídico que se utiliza, para mantener o restituir el goce o disfrute de los derechos o garantías que la constitución establece”*, incluidas las acciones de Hábeas Data y Hábeas Corpus. Con lo cual se establece que el Hábeas Data y Hábeas corpus desde el punto de vista procesal constituyen una especie de amparo específico dentro del régimen jurídico de amparo genérico hondureño.

En otros ámbitos latinoamericanos como el argentino por ejemplo, la doctrina acude a la acción exhibitoria de los datos personales no como un fin sino como un resultado del derecho que le asiste a *“toda persona —identificada o identificable— a solicitar judicialmente la exhibición de los registros —públicos o privados—, en los cuales están incluidos sus datos personales o los de su grupo familiar, para tomar conocimiento de su exactitud; a requerir la rectificación, la supresión de datos inexactos u obsoletos o que impliquen discriminación”* ^[73].

2.4.6. El Hábeas Data es un derecho humano de “tercera generación”

Los derechos humanos en todo tiempo, lugar y clasificación siguen siendo derechos del ser humano que identifican, definen y diferencian inequívocamente a la especie humana de cualquiera otra. Por ello, cuando hablamos de derechos de primera, segunda o tercera generación daría la impresión que existen derechos humanos clasificados peyorativamente o con grados de mejor o peor valer. Esto no es así. Los derechos humanos en una u otra generación no cambian su connotación, su eficacia, su

(72) URIOSTE, Mercedes. **Protección de datos personales**. En: <http://www.derecho-comparado.com>

(73) Ekmekdjian, Miguel Á. y Pizzolo, Calogero, **“Hábeas Data”**, citado por GORDILLO J.F et all. Ob., ut supra cit.

Esencia en la dignidad y el respeto mutuo humanos y sus efectos para todos, sea niños, adultos, hombres o mujeres, blancos o negros, “discapacitados” o normales física y síquicamente, etc.

Hoy por hoy, existe un consenso universal sobre los motivos y razones históricas, políticas, económicas, culturales y jurídicas en las cuales se gestaron los derechos humanos de primera, segunda y tercera generación. Sobre éstos últimos se dice que surgieron “en los años 70, cuando los países “en desarrollo” reclaman gozar de verdad del derecho a la autodeterminación”^[74]. Si el reconocimiento de los derechos de primera generación --los derechos de la libertad--, llevó a descubrir los derechos de segunda generación --derechos de la igualdad--, éstos han llevado a descubrir los derechos de tercera generación, cuyo valor fundamental de referencia es la solidaridad”^[75] de la comunidad, de los pueblos o de los Estados tanto en los amenazantes problemas globales (medio ambiente, industrialización con alta y peligrosa tecnología, el abuso o mala utilización de las nuevas tecnologías de la información y la comunicación o medios TIC), como en las mecanismos más eficientes e idóneos para la solución de aquellos, tales como la suscripción entre Estados de Tratados, Convenios, Acuerdos o Recomendaciones Internacionales con fines sociales, culturales, económicos y científicos; adoptar medidas tecnológicas mundiales para reducir al máximo con los elementos altamente contaminantes de agua, aire, plantas, animales e incluso al ser humano; adoptar medidas tecnológicas globales para bien utilizar los medios TIC y la informática.

“Los derechos humanos de tercera generación pretenden partir de la totalidad de necesidades e intereses del ser humano tal como se manifiestan en la actualidad. Si el titular de los derechos de primera generación era el ser humano aislado, y los protagonistas de los derechos de segunda generación eran los seres humanos en grupos, las nuevas circunstancias actuales exigen que la titularidad de los derechos corresponda, solidaria y universalmente, a todos los hombres. El individuo y los grupos resultan insuficientes para responder a las agresiones actuales que afectan a toda la humanidad”^[76].

Uno de los nuevos derechos fundamentales surgidos en el ambiente de la tercera generación es precisamente el Hábeas Data, ya que éste crea el derecho o “libertad de autodeterminación” o control de los datos personales que le conciernen y se hayan recabado en bancos de datos públicos o privados. El indebido, ilegítimo o ilegal uso y utilización de los medios TIC y de la informática provocaron en sus inicios serias amenazas a los derechos fundamentales de la intimidad^[77], el honor, la buena imagen, el buen nombre, la reputación; entre otros. Por estas razones los Estados Europeos desde la década de los años setenta y ochenta comenzaron a emitir recomendaciones y convenios internacionales como los de la OCDE de 1980 o el Convenio de Estrasburgo de

(74) En: <http://www.iglhrc.org/>

(75) BAIGORRI, José, et all. **Los Derechos Humanos** En: <http://www.amnistiacatalunya.org/edu/>

(76) BAIGORRI, José, et all. **Los Derechos** Ob., ut supra cit.

(77) Esta postura unidimensional solo contra la “privacidad” o intimidad de las personas generó la constitucionalización y posterior reglamentación legislativa del Hábeas Data en Latinoamérica, a partir de 1988. Así se revela en los siguientes apartes: “El avance de la tecnología y de las telecomunicaciones ha ocasionado el surgimiento de nuevas formas de intromisión a la intimidad de las personas, así como la multiplicación del efecto de las intromisiones realizadas conforme a mecanismos ya existentes. Por esto surgió la institución jurídica del Hábeas Data por medio del cual los particulares pueden conseguir una tutela efectiva de su derecho a la intimidad, desde luego esta no es la única institución jurídica concebida para este fin, ni excluye la posibilidad de intentar otras acciones”. Cfr. VELÁSQUEZ V., Santiago. **El derecho a la Intimidad y la competencia desleal**. En: <http://www.revistajuridicaonline.com/>

1981, para proteger los derechos y libertades constitucionales de la persona humana, principalmente la “privacidad” (o derecho a la intimidad) contra el “flujo internacional de datos” indiscriminado, no autorizado o sin utilización y finalidad predefinidos. En América, los 21 Estados fundadores de la Organización de Estados Americanos, O.E.A. (fundada el 30 de Abril de 1948, en la IX Conferencia Panamericana en la que se suscribió el Pacto de Bogotá) emitieron recomendaciones y normas internacionales, como la Declaración Universal de los derechos Humanos y a partir de ésta el Pacto Sectorial sobre derechos civiles y políticos (incorporado al derecho interno colombiano, mediante la Ley 74 de 1968) y el Convenio Sectorial de Derechos Humanos o Pacto de San José de Costa Rica (Incorporado al derecho colombiano, mediante la Ley 16 de 1972). En estas normas universales y sectoriales se estipularon derechos para proteger al ser humano en su “privacidad” o intimidad, el derecho a la información, a la libertad de pensamiento, opinión y expresión, al honor, entre otros muchos ^[78].

Para Pérez Luño con visión europeísta más que latinoamericana sostiene que, “*El hábeas data constituye un cauce procesal para salvaguardar la libertad de la persona en la esfera informática, que cumple una función paralela, en el seno de los derechos humanos de la tercera generación, a la que en los de primera generación correspondió al hábeas corpus respecto a la libertad física o de movimientos de la persona... Al cotejar el hábeas corpus y el hábeas data se comprueba una inicial coincidencia en lo referente a su naturaleza jurídica. En ambos casos no se trata de derechos fundamentales, stricto sensu, sino de instrumentos o garantías procesales de defensa de los derechos a la libertad personal, en el caso del hábeas corpus, y de la libertad informática en lo concerniente al hábeas data*”^[79]. Dijimos visión europeísta, porque el tratadista compara la acción del Hábeas Data con la acción de la protección de datos y ésta en el derecho ibérico principalmente se cataloga como una emanación de la “libertad informática” y por tanto su naturaleza jurídica pertenece a las libertades constitucionales y no a los derechos igualmente constitucionales. En el ámbito Latinoamericano como hemos visto anteriormente, el Hábeas Data ha sido calificado como derecho autónomo y fundamental, garantía constitucional, recurso o acción constitucional e incluso proceso constitucional en el ambiente argentino, peruano y ecuatoriano, pero en manera alguna como una libertad constitucional.

3. ELEMENTOS QUE COMPONEN EL HABEAS DATA

En este aparte, más con sentido académico que con otra finalidad jurídica haremos una división y descripción de los que hemos llamado elementos subjetivos, objetivos y formales del Hábeas Data, pues estos nos permitirán hacer alusión a varias de las definiciones técnico-jurídicas esenciales en el tratamiento de datos informatizado o no de datos, así como a los aspectos de legitimidad por activa y por pasiva del Hábeas data como acción procesal en un eventual proceso jurisdiccional de amparo o tutela específico, o bien en un proceso de carácter administrativo ante responsables de la administración y manejo de los bancos de datos públicos o privados, “centrales de información” financiera (crediticia, bancaria, tarifaria, etc.), o también ante organismos o entidades de control y vigilancia de los bancos de datos o centrales de información general o especializada.

Igualmente la determinación de los elementos objetivos o materiales que componen el

(78) RIASCOS GOMEZ, Libardo O. *El derecho a la Intimidad, la visión ius-informática y los delitos relativos a los datos personales*. Tesis doctoral, Universidad de Lleida (España), Lleida, 1999, pág. 15 y ss.

(79) PEREZ LUÑO, Antonio Enrique, *Ensayos de informática jurídica*, México, Distribuciones Fontamara, 1996, pp. 14 y 15.

Hábeas Data nos permitirá estudiar el dato o información personal como de la esencial del bien jurídico tutelado por las leyes protectoras de los datos personales, leyes protectoras del Hábeas Data, leyes protectoras del dato financiero o leyes protectoras del derecho de acceso a la información o la transparencia de la gestión pública, según el Estado y el nomen iuris adoptado por éste para proteger los mentados datos personales.

3.1. Elementos subjetivos

De la conceptualización generalizada del Hábeas data como derecho y como garantía constitucional, suministrada ut supra, se puede deducir que los sujetos que intervienen en su estructuración están los titulares de los datos, los causahabientes o sucesores, El Estado como persona jurídica de derecho público y los responsables de los bancos de datos públicos o privados, o de “las centrales de información” financiera (crediticia, bancaria, bursátil, tributaria, tarifaria, etc.,) o especializada.

3.1.1. El Titular de los datos

El Hábeas Data en el ámbito latinoamericano es un derecho constitucional aforado a “*toda persona*” que tiene como facultades prioritarias, en principio el acceso y conocimiento de la información o datos personales que a ella le conciernen, y luego según la aprehensión de este conocimiento, si observa que los datos son inexactos, incompletos, erróneos, “antiguos”, falsos, “discriminatorios” o no conformes a derecho, podrá solicitar ante las personas, autoridades públicas o privadas, en vía administrativa o vía jurisdiccional, según el Estado latinoamericano y las reglas de competencia por éstos establecidas: la actualización, la rectificación, la eliminación o la “anulación” de los datos personales.

La Ley 1266 de 2008, en el artículo 3º literal a, define al “titular de la información”, así: “*Es la persona natural o jurídica a quien se refiere la información que reposa en un banco de datos y sujeto del derecho de hábeas data y demás derechos y garantías a que se refiere la presente ley*”.

3.1.1.1. Las personas físicas, naturales o humanas

En el contexto de las Constituciones Latinoamericanas y las correspondientes leyes reglamentarias del derecho de Hábeas Data en forma inequívoca se confiere la titularidad de los datos personales a toda persona, *ab initio*, natural, física o humana determinada o determinable, pues no cabe la titularidad de los datos para una persona anónima. La titularidad evoca un claro derecho de propiedad inmaterial sobre el dato, además de las facultades o derechos inherentes al Hábeas data: acceso, conocimiento, actualización, rectificación y eliminación datos personales recabados en bancos, registros, bases o ficheros de datos o informaciones personales, sean de naturaleza pública o privada.

3.1.1.2. Las personas jurídicas, morales o de “existencia ideal”

Aunque en principio se discutió la titularidad de datos personales por parte de las personas jurídicas, morales o de “existencia ideal” (como se le denomina en el derecho argentino, uruguayo y del Paraguay), muy pronto se desistió de la tesis negativa, por las siguientes razones: (i) la persona jurídica, al igual que la persona física, es titular de derechos y obligaciones en el derecho universal; (ii) Los textos constitucionales y leyes latinoamericanas, al reglamentar la institución jurídica del Hábeas Data (como acción, recurso, garantía o proceso) lo hace recaer en “toda persona”, como del titular de los datos personales, sin hacer distinción alguna sobre su naturaleza jurídica (humana o

moral), el sexo, la nacionalidad, el domicilio e incluso la edad cronológica (desde el *nasciturus* por vía excepcional tendría titularidad en éste derecho); y, (iii) Aunque algunos derechos inherentes a la persona humana, como el de la intimidad por ejemplo, no serían los tutelados cuando se solicita la protección de datos de la persona jurídica, sí podría eventualmente solicitarse la tutela del derecho a la *“identidad o a la buena imagen”* porque en éste caso, *“el Hábeas Data protege un derecho a la verdad sobre los datos sociales que se posean en un determinado registro y que hagan a la reputación fama y buen nombre del afectado”* ^[80].

3.1.1.3. Personas humanas y jurídicas. Excepciones.

La Ley Nacional de Protección de datos de la Argentina de 2000 en el artículo 2º, inciso 7º, y en similar sentido varias leyes Latinoamericanas sobre el particular, reconoce expresamente que es titular de los datos personales, *“toda persona física o persona de existencia ideal (o jurídicas) con domicilio legal o delegaciones o sucursales en el país, cuyos datos sean objeto del tratamiento de datos”*. En cambio, la Ley No. 19.628 de 1999, relativa a la *“protección de la vida privada o protección de datos de carácter personal”*, al prever como bien jurídico tutelado sólo a la privacidad o la intimidad de las personas, arroga la titularidad del derecho de Hábeas data a la persona física en el artículo 2º -ñ, así: *“Titular de los datos, la persona natural a la que se refieren los datos de carácter personal”* ^[81].

Este proceder de la legislación Chilena es coherente porque la ley solo protege el derecho a la intimidad individual y familiar de las personas, al igual que lo siguen haciendo las leyes de protección de datos personales de Europa, tanto las nacionales (caso de España ^[82], Portugal, Francia, Alemania) como las comunitarias (Recomendaciones de OCDE y Convenio de Estrasburgo de 1980 y 1981, respectivamente y las Directivas 95/46/CE y 97/66/CE). En todas ellas el titular de los datos es el *“afectado o interesado”* con los datos personales, que sólo puede serlo la persona natural o física.

La Ley Federal Alemana de protección de datos de 1976-1994 o LFAPD, consecuentemente con lo anterior y al hacer mención a la persona humana como titular de los datos, en el *“proceso”* o tratamiento de datos, hace expresa referencia a los derechos derivados del acceso y consulta de la información. Estos derechos son: (i) La información acerca de los datos almacenados en relación con la persona; (ii) La Rectificación de los datos almacenados en relación con su persona, cuando los mismos fueren inexactos; (iii) El bloqueo de los datos almacenados en relación con su persona cuando no pudiere determinarse su exactitud o inexactitud, o cuando dejaren de darse las condiciones que originariamente requirieran su almacenamiento; y (iv) La cancelación de los datos almacenados en relación con su persona, si su almacenamiento no había sido admisible o bien --a elección, además del derecho de cancelación-- cuando dejaren de darse las condiciones que originariamente requirieran su almacenamiento.

Tanto las personas humanas como jurídicas están legitimadas para incoar una acción, recurso o garantía de Hábeas Data en un proceso jurisdiccional o administrativo, bien sea

(80) PALAZZI, Pablo. *El Hábeas Data en el derecho argentino*. Revista de Derecho Informático. ISSN 1681-5726. Ed. Alfa-Redi, No. 04, Noviembre de 1998.

(81) AA.VV. *Ley sobre protección a la vida privada o protección de datos de carácter personal*. En: <http://www.sernac.cl/leyes/>

(82) **Afectado o interesado:** Persona física titular de los datos que sean objeto del tratamiento de datos respectivo, según la Ley Orgánica de protección de Datos No. 15 de Diciembre 23 de 1999 o LOPDP

en forma directa, a través de apoderado judicial o mediante el representante legal de la entidad, organismo o dependencia pública o privada, según fuere el caso y clase de persona.

En los proyectos de ley estatutaria del Hábeas Data en Colombia, encontramos la corriente latinoamericana y no europea respecto de los titulares de los datos. En efecto, en el proyecto de Ley No. 64 de 2003, *“por el cual se dictan disposiciones para la protección de datos personales y se regula la actividad de recolección, almacenamiento y circulación de datos”*, se determina que es *“Titular del dato personal...toda persona natural o jurídica, pública o privada a quien se refiere la información que reposa en un banco de datos o central de la información”*.

En sentido similar, el proyecto de ley estatutaria No. 071 de 2005 *“por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera y crediticia, y se dictan otras disposiciones”*, cambia el término de “datos” por “información”, para concluir diciendo que el *“Titular de la Información...Es la persona natural o jurídica, a quien se refiere la información que reposa en un banco de datos y sujeto del derecho de hábeas data y demás derechos y garantías a que se refiere la...ley”*. En idéntico sentido el último proyecto de Hábeas Data presentado al Congreso de la República en el año de 2006 y que hasta la fecha no se ha convertido en ley. Es el proyecto de Ley Estatutaria No. 211/2007 Cámara, No. 027/2006 Senado, acumulado con el No. 05/2006 Senado, *“Por el cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial y de servicios...”*

La Ley de Habeas Data financiero de 2008, terminó adoptando la definición de titular de la información prevista en el proyecto de ley estatutaria de 2005, como *ut supra* se transcribió.

3.1.1.4. El “afectado”, “cualquier persona”, las organizaciones con fines e intereses colectivos y el Defensor del Pueblo están legitimados para incoar el Hábeas data colectivo.

En el derecho argentino se planteo la posibilidad de *“ejercer una suerte de Hábeas Data colectivo en los casos de discriminación”* ^[83] previsto en el inciso 2º del artículo 43 de la Constitución por parte del *“afectado, el defensor del pueblo y las organizaciones que propendan por esos fines”* (protección al ambiente, a la competencia, al usuario y al consumidor, así como a los derechos de incidencia colectiva en general). Estos estarían legitimados por activa para proponer la acción de Hábeas Data en interés colectivo cuando

en un banco o tratamiento de datos personales se amenace o vulnere un derecho fundamental con cualquier forma de discriminación.

En el derecho colombiano el proyecto de Ley estatutaria de Hábeas Data de 2005, a instancias de la Defensoría del Pueblo, mencionó por vez primera *“el Hábeas Data colectivo”* o *“de interés público”* ejercitable, según los artículos 3-4 y 24, por *“cualquier persona, organización o al defensor del pueblo”*, para *“solicitar la suspensión, rectificación o cesación de un tratamiento de datos que se está realizando de manera*

(83) PALAZZI, Pablo. *El Hábeas Data en el derecho...* Ob., ut supra cit.

irregular, con pretermisión de los requisitos establecidos para ello, o respecto de datos que no pueden ser objeto de tratamiento o cuyo tratamiento está sujeto a condiciones o requisitos que no se han cumplido y que afecta a una generalidad o grupo de personas determinadas o no". Habeas data colectivo que no puede interpretarse o confundirse con las acciones de grupo o popular constitucional prevista en nuestra Constitución en el artículo 88 y reglamentada en la Ley 472 de 1998, pues aunque el fundamento de unas y otras son los derechos de la colectividad, "la generalidad" o la comunidad, el objetivo específico del Hábeas Data colectivo se dirige exclusivamente a restringir, limitar o prohibir un tratamiento o procesamiento de datos personales informatizado o no que amenace o vulnere derechos constitucionales o legales de esa colectividad.

La Ley de Habeas Data financiero de 2008, se abstuvo inexplicablemente de hacer siquiera mención al habeas data colectivo a instancia de una organización o de la defensoría del Pueblo. La principal razón es que esta ley no tiene sujetos activos ni pasivos colectivos, es exageradamente individualista porque se entiende que el titular de los datos sólo puede ser una persona natural o jurídica.

3.1.1.5. "Curadores o tutores del afectado" y los causahabientes

La LPD Argentina de 2000, en el artículo 34, al mencionar la legitimación por activa de la acción de protección de datos personales o de Hábeas Data, sostiene que podrá ser ejercitada además del "afectado" o titular de los datos, por "sus curadores o tutores", es decir, por las personas elegidas o nombradas para cuidar los bienes o negocios de un menor de edad, o de quien no estaba en estado de administrarlos por sí.

El proyecto de ley estatutaria colombiana de Hábeas Data de 2005, a instancia de la Defensoría del Pueblo, preveía un trato jurídico especial para los menores de edad que estuviesen involucrados en un tratamiento o procesamiento de datos o más aún cuando ya estuviesen recabados en una base o banco de datos, pues en el artículo 7º manifestaba que *"el tratamiento, uso, transmisión o divulgación de datos se asegurará el respeto a los derechos prevalentes de los niños"*; agregaba en el inciso 2º, *"El tratamiento de datos de carácter personal de menores sólo podrá hacerse con fines institucionales autorizados por la ley"*; y finalizaba en el inciso 3º proscribiendo "el tratamiento, uso, divulgación, publicación o circulación de datos de carácter personal de menores cuyo fin sea su comercialización, tráfico, venta o cesión a terceros, excepto cuando se trate de información sobre solvencia patrimonial o financiera de menores adultos requerida en desarrollo de contratos de la misma índole para los cuales se encuentre habilitado por ley.

De lo anterior se deduce que en el evento que pudiese estar involucrado un menor de edad en un tratamiento o procesamiento de datos personales y con éste se afecte, amenace o vulnere derechos constitucionales o legales, éste como titular de los datos podrá a través de sus padres, o de su tutor o curador nombrado o designado al efecto, o mediante apoderado judicial, ejercitar la acción de Hábeas Data.

Respecto al término "causahabiente", utilizado por varias leyes Latinoamericanas de protección de los datos personales, o también reglamentaria del Hábeas data; así como en el proyecto de Ley Estatutaria colombiano de 2003 y 2007 de iniciativa de la defensoría pública y de origen gubernamental y parlamentario, respectivamente, lo hacen en el sentido lato o amplio, es decir, que causahabiente genéricamente se denomina a "cualquier persona que deriva el todo o parte de sus derechos de otra que se llama su "autor" o "causante". Si la derivación se verifica por un acto entre vivos se denomina

transferencia y si se verifica por causa de muerte, transmisión, la que puede ser a título universal o a título singular.

De suerte, entonces, que son terceros relativos los herederos y legatarios de alguna de las partes y los cesionarios de ellas, todos los cuales son causahabientes.

Los sucesores o causahabientes reciben el derecho de su causante o autor en las mismas condiciones en que éste lo tenía, es decir, el derecho pasa de causante a sucesor con las mismas ventajas y cargas.

Los sucesores o causahabientes a título singular sufren los efectos de los actos realizados por su causante solo en relación con la cosa o derecho que se les ha transferido o transmitido.

Los sucesores o causahabientes a título universal, en cambio, les afectan todos los actos de su causante, todos los actos les aprovecha o perjudica; todos los derechos adquiridos por su autor, salvo los personalísimos; y deben cumplir todas sus obligaciones”^[84].

El proyecto de ley No. 064 de 2003, al definir al “titular de la información” manifestaba que ostentaba esta calidad la persona a la quien le conciernen los datos y “sus causahabientes” quienes “gozan también de legitimidad para el ejercicio de los derechos y acciones correspondientes” al Hábeas Data.

El Proyecto de Ley Estatutaria de 2007, sin mencionar expresamente en la definición de “titular de la información” a los causahabientes, en el contexto del proyecto hace referencia a los derechos que éstos tienen en todas las etapas del tratamiento o procesamiento de la información o datos personales, en las mismas condiciones y formalidades que los titulares de la información o datos. V.gr. en la “circulación de información”, artículo 5º; así como también en el trámite del Hábeas Data administrativo colombiano, originado por peticiones, consultas o reclamos ante las autoridades de control o los responsables de los bancos de datos o “centrales de información” financiera o especializada (artículo 16 del proyecto).

De lo anterior se infiere entonces que los causahabientes son titulares de los datos por transferencia o transmisión de su autor o causante y por lo tanto, está legitimado por activa para ejercer los derechos o facultades del Hábeas Data.

La Ley de Habeas Data financiero de 2008, no reparó en estos temas puntuales, puesto que son labores del operador jurídico o del intérprete de la ley, entender que todos cabrían dentro del concepto genérico de persona como titular de la información. Sin embargo, al igual que el proyecto de Ley Estatutaria acumulado de 2006-2007, hizo referencia a los causahabientes en los principios que rigen en la administración de los datos, tales como el de circulación restringida de los datos (artículo 5º, literal a,); en el trámite de las consultas de la información realizadas por los titulares de la información o sus causahabientes (artículo 16º, numeral I,) como también en el trámite de reclamos respectivos (artículo 16, numeral II).

3.1.1.6. El Estado

En el término más universalmente conocido, el estado es la persona jurídica de derecho público que puede adquirir derechos y contraer obligaciones. En tal virtud, los organismos,

(84) AA.VV. *Teoría general del contrato*. En: <http://www.udp.cl/derecho/>

dependencias o entidades que hacen parte del estado en tal estén representadas legal, estatutaria o legítimamente, podrán ser eventualmente titulares de datos que éstas les conciernan y estarán legitimadas para ejercitar algunas de las facultades o derechos componentes del Hábeas Data, pero obviamente no en defensa y protección del derecho a la intimidad como derecho personalísimo exclusivo de las personas naturales o físicas, como anteriormente hemos sostenido.

Estos organismos, entidades o dependencias del Estado están legitimados en esta clase de asuntos del Hábeas Data, tanto por activa como por pasiva, según si son titulares de los datos personales o por el contrario son responsables, administradores o manejadores de los bancos de datos públicos, o centrales de información financiera o especializada de carácter público.

Según Palazzi ^[85], al plantear la posibilidad de que el Estado sea “el actor en un proceso de Hábeas Data”, será posible, “*cuando éste actúe en el campo del derecho privado. Pensamos que para que ello suceda, el Estado, o quien lo represente, debería estar registrado en un banco o base de datos, o al menos existir un determinado dato, o una información a la que se pretenda acceder*”. Y agrega, “*Recordemos que el artículo 43 establece un derecho de acceso y control de la información que puede ser ejercido en forma independiente del derecho de rectificar o actualizar esa información*”.

De esta forma, el autor citado parece plantear que el Estado sólo podría ejercitar las facultades del Hábeas Data de acceso y conocimiento de la información o datos y excluye las facultades de actualización, rectificación y cancelación de datos. Teóricamente es posible ejercitar todas las facultades del Hábeas data así sea el titular una persona jurídica.

3.1.2. Los responsables del tratamiento, banco o registro de datos, “Centrales de información” financiera o especializada, los “Operadores de los Datos”, los fuente-operador de información y “Las Agencias de información comercial”

Las definiciones son sinónimas en el concepto de ser personas naturales o jurídicas, públicas o privadas que administran, manejan, dirigen o son responsables de los bancos de datos personales públicos o privados y constituyen se constituyen como “sujetos pasivos” del tratamiento informatizado o no de datos, en otros términos, son los sujetos legitimados por pasiva. Se diferencian, en atención al Estado donde se aplican dichas denominaciones, así como en algunas funciones especiales y en las leyes que les dan origen: unas, por las leyes de protección de datos; y otras, por leyes reguladoras del Hábeas Data integral, general o sectorial.

La Ley Orgánica de Protección de datos de España o LOPDP de 1999, en el artículo 3-d, define al “Responsable del fichero o tratamiento”, como la “*persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento*”.

En la definición se destaca la naturaleza y titularidad jurídica de las personas que realizan el tratamiento de datos personales y sobre todo la finalidad, contenido y uso del mismo.

En la legislación argentina, LPDA de 2000, se define al “*Responsable del archivo, registro, base o banco de datos*”, como la “*persona física o de existencia ideal pública o privada, que es el titular de un archivo, registro, base o banco de datos*”

(85) PALAZZI, Pablo. *El Hábeas Data en el derecho...* Ob., ut supra cit.

En esta definición se parte del sinónimo de archivo, registro, base o banco de datos entendido solo en el tratamiento informatizado o no de datos personales, para luego hacer énfasis en la titularidad pública o privada de dicho tratamiento y la persona que administra, dirige o es responsable de aquél.

Por su parte el proyecto de Ley estatutaria colombiana de Hábeas Data No. 064 de 2003, definía al “Responsable del tratamiento”, como “*la persona natural o jurídica, pública o privada, o el servicio u organismo que trata datos personales por cuenta del operador del banco de datos o de la central de la información*”. Se partía del ejemplo extranjero europeo y latinoamericano sobre el responsable del tratamiento de los datos o del “fichero” o banco de datos, para luego incorporar en dicha definición también a los denominados “operadores de los bancos o de la central de información”. Esto por cuanto en Colombia son las organizaciones privadas con servicios financieros, como la “Central de Información” de la Asociación bancaria y de entidades financieras de Colombia – CIFIN-^[86], DataCrédito^[87], Covinoc, Computec, Inconcrédito, Credicheque, Fenalcheque, etc. “*sociedades o agremiaciones de carácter privado en las cuales se registra el comportamiento crediticio, financiero y comercial de las personas que celebran operaciones con entidades financieras, cooperativas y empresas de sector real*”^[88] y son las que han dominado el mercado de la información crediticia y bancaria en Colombia, por varios años y las que han generado gran parte de la jurisprudencia de la Corte Constitucional en materia del dato financiero en nuestro país. En el derecho comparado coexisten entidades u organismos de información financiera de carácter privado con las de naturaleza pública (v.gr. En el derecho argentino “La Central de Deudores del Sistema Financiero” como sistema de información crediticia del Banco Central de la República Argentina, B.C.R.A.)^[89].

(86) **CIFIN** “es un servicio de recolección, almacenamiento, procesamiento, administración, divulgación y cesión de información, conformado por bases de datos de diverso carácter, a través de las cuales se muestra el comportamiento comercial y financiero de las personas que son reportadas a ellas. **¿Para qué sirve?** La actividad crediticia implica riesgo y por tanto requiere que quien vaya a conceder crédito actúe con prudencia y tome las mayores precauciones, a fin de evitar la pérdida de los dineros prestados. La principal precaución consiste en conocer el perfil de riesgo del futuro deudor. (...) Debe resaltarse que la información que reposa en CIFIN no sólo es necesaria para la concesión del crédito sino para determinar su riesgo una vez concedido este. Es por ello que la Circular Externa 100 de 1995 la Superintendencia Financiera establece que uno de los criterios de evaluación de la cartera, es la “información proveniente de centrales de riesgos, consolidadas con el sistema, y de las demás fuentes de información comercial de que disponga la institución vigilada”.
En: <http://cifin.asobancaria.com>

(87) **DATA CREDITO**. “Es una central de información financiera. *Naturaleza*. Es la recopilación sistematizada y organizada de datos de carácter crediticio, que permite tomar decisiones tendientes a determinar el riesgo de crédito. Los bancos de datos de información crediticia, recopilan y muestran la historia de comportamiento de pago de personas y empresas incluyendo tanto los pagos oportunos como los retrasos. La existencia de las centrales de información se encuentra amparada en la libertad de empresa, la libre iniciativa privada y el ejercicio del derecho a la información. **Principios:** (i) Calidad de la información: Veraz, exacta, actualizada, comprobable y comprensible; (ii) Relevancia de la información: Permanencia de la información; (iii) Libre acceso al ciudadano: conocer, actualizar y rectificar; (iv) Seguridad de la información: evitar adulteración, pérdida o uso no autorizado; y (v) Respeto de los derechos constitucionales: Información, Buen nombre y Hábeas Data”. Es importante destacar que DataCrédito expidió su Código de Conducta, en “el cual se recopila la forma como debe funcionar su base de datos con el fin de garantizar tanto la protección de derechos de los ciudadanos como la calidad de la información”. En: www.datacredito.org.co

(88) En: <http://www.superfinanciera.gov.co/GuiasInformativas/educa-centralesriesgo.htm>

(89) La central es un servicio de información del B.C.R.A, a través de la superintendencia de entidades financieras y cambiarias. Se ha estructurado en base a los datos que proveen las entidades financieras, las entidades no financieras emisoras de tarjetas de crédito y el propio B.C.R.A. Tiene por objeto brindar información sobre los deudores del sistema financiero a los bancos y demás instituciones que intermedian en el crédito, para facilitar la toma de decisiones en materia crediticia”. LIVELLARA, Silvina. **Hábeas Data e información crediticia. La eventual responsabilidad civil de las entidades financieras y del banco central de la República Argentina por cesión y publicidad de datos inexactos**. Vía Internet.

Finalmente, el proyecto de ley estatutaria colombiana de Hábeas Data sectorial de 2006 y 2007, la nominación de “responsables del tratamiento”, “responsables de los bancos de datos”, “responsables del tratamiento o bancos de datos por cuenta de un tercero: el operador” o los “responsables de las centrales de información” para unificarlos en uno sólo omnicompreensivo de todos los anteriores: “El Operador de la Información”.

En efecto, en el artículo 3-c, del proyecto de ley define al “Operador de información”, como “*la persona, entidad u organización que recibe de la fuente datos personales sobre varios titulares de la información, los administra y los pone en conocimiento de los usuarios bajo los parámetros de la presente ley. Por tanto el operador, en cuanto tiene acceso a información personal de terceros, se sujeta al cumplimiento de los deberes y responsabilidades previstos para garantizar la protección de los derechos del titular de los datos. Salvo que el operador sea la misma fuente de la información, este no tiene relación comercial o de servicio con el titular y por ende no es responsable por la calidad de los datos que le sean suministrados por la fuente*”^[90].

Los titulares de los datos o la información, entre otros derechos reconocidos por el proyecto de ley de 2006-2007, tendrán los siguientes derechos frente a los operadores de los bancos de datos: (i) Ejercer el derecho fundamental al hábeas data en los términos de la presente ley, mediante la utilización de los procedimientos de consultas o reclamos, sin perjuicio de los demás mecanismos constitucionales y legales; (ii) Solicitar el respeto y la protección de los demás derechos constitucionales o legales, así como de las demás disposiciones de la presente ley, mediante la utilización del procedimiento de reclamos y peticiones; (iii) Solicitar prueba de la certificación de la existencia de la autorización expedida por la fuente o por el usuario; (iv) Solicitar información acerca de los usuarios autorizados para obtener información.

Se aclara sobre estos derechos que: (i) La administración de información pública no requiere autorización del titular de los datos, pero se sujeta al cumplimiento de los principios de la administración de datos personales y proyecto de ley; y (ii) La administración de datos semi-privados y privados requiere el consentimiento previo y expreso del titular de los datos, salvo en el caso del dato financiero y crediticio, el cual no requiere autorización del titular. En todo caso, la administración de datos semi-privados y privados se sujeta al cumplimiento de los principios de la administración de datos personales y a las demás disposiciones de ley.

La Ley de Habeas Data de 2008, retomó en su integridad las conceptualizaciones anteriores y las plasmó en el artículo 3º, literales b), c), i) y j). Así mismo, respecto de los derechos que tienen los titulares de los datos frente a los operadores de información (artículo 6º, numeral 1º y parágrafo).

Estableció además los deberes de los operadores de la información en los bancos de datos en el artículo 7º de la Ley 1266 de 2008, así: 1. Garantizar, en todo tiempo al titular de la información, el pleno y efectivo ejercicio del derecho de hábeas data y de petición,

(90) La Corte Constitucional mediante **Sentencia C-1011-2008**, declaró constitucional el mentado artículo en forma condicionada, así: “**Tercero.-** Declarar **EXEQUIBLE** el artículo 3º del Proyecto de Ley objeto de revisión, en el entendido que respecto a lo previsto en el literal c) de este artículo, el operador es responsable a partir de la recepción del dato suministrado por la fuente, por el incumplimiento de los deberes de diligencia y cuidado en relación con la calidad de la información personal, consagrados en esta Ley Estatutaria. Esta declaratoria de exequibilidad operará salvo la expresión “*así como la información relativa a las demás actividades propias del sector financiero o sobre el manejo financiero o los estados financieros del titular*”, contenida en el literal j) del artículo 3º del Proyecto de Ley Estatutaria, que se declara **INEXEQUIBLE**”.

es decir, la posibilidad de conocer la información que sobre él exista o repose en el banco de datos, y solicitar la actualización o corrección de datos, todo lo cual se realizará por conducto de los mecanismos de consultas o reclamos, conforme lo previsto en la presente ley; 2. Garantizar, que en la recolección, tratamiento y circulación de datos, se respetarán los demás derechos consagrados en la ley; 3. Permitir el acceso a la información únicamente a las personas que, de conformidad con lo previsto en esta ley, pueden tener acceso a ella; 4. Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y, en especial, para la atención de consultas y reclamos por parte de los titulares; 5. Solicitar la certificación a la fuente de la existencia de la autorización otorgada por el titular, cuando dicha autorización sea necesaria, conforme lo previsto en la presente ley; 6. Conservar con las debidas seguridades los registros almacenados para impedir su deterioro, pérdida, alteración, uso no autorizado o fraudulento; 7. Realizar periódica y oportunamente la actualización y rectificación de los datos, cada vez que le reporten novedades las fuentes, en los términos de la presente ley; 8. Tramitar las peticiones, consultas y los reclamos formulados por los titulares de la información, en los términos señalados en la presente ley; 9. Indicar en el respectivo registro individual que determinada información se encuentra en discusión por parte de su titular, cuando se haya presentado la solicitud de rectificación o actualización de la misma y no haya finalizado dicho trámite, en la forma en que se regula en la presente ley; 10. Circular la información a los usuarios dentro de los parámetros de la presente ley; 11. Cumplir las instrucciones y requerimientos que la autoridad de vigilancia imparta en relación con el cumplimiento de la presente ley; y, 12. Los demás que se deriven de la Constitución o de la presente ley.

3.1.2.1. Fuentes de Información y los “fuente-operadores” de información financiera

El artículo 3, literal j, de la Ley de Protección de datos personales de España, como norma integral del “Hábeas Data”, se ocupa al igual que la LPDA argentina de 2000, principalmente por determinar las fuentes accesibles al público, las cuales las denomina como *“aquellos ficheros cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa, o sin más exigencia que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público, los Diarios y Boletines oficiales y los medios de comunicación”*.

En cambio el proyecto de ley estatutaria colombiano del Hábeas Data de 2006-2007 enfatiza en el concepto de fuente de información de carácter financiero, bien si actúa como tal o lo hace en forma sui géneris, como fuente-operador. En efecto, según el literal b, del artículo 3º del proyecto se entiende como *“Fuente de información,... la persona, entidad u organización que recibe o conoce datos personales de los titulares de la información, en virtud de una relación comercial o de servicio o de cualquier otra índole y que, en razón de autorización legal o del titular, suministra esos datos a un operador de información, el que a su vez los entregará al usuario final. Si la fuente entrega la información directamente a los usuarios y no, a través de un operador, aquella tendrá la doble condición de fuente y operador y asumirá los deberes y responsabilidades de ambos. La fuente de la información responde por la calidad de los datos suministrados al operador la cual, en cuanto tiene acceso y suministra información personal de terceros, se*

sujeta al cumplimiento de los deberes y responsabilidades previstas para garantizar la protección de los derechos del titular de los datos”.

Según el proyecto de ley estatutaria colombiana de Hábeas Data 2006-2007, el titular de los datos personales tiene los siguientes derechos frente a las fuentes de información: (i) Ejercer los derechos fundamentales al hábeas data y de petición, cuyo cumplimiento se podrá realizar a través de los operadores, conforme lo previsto en los procedimientos de consultas y reclamos de esta ley, sin perjuicio de los demás mecanismos constitucionales o legales; (ii) Solicitar información o pedir la actualización o rectificación de los datos contenidos en la base de datos, lo cual realizará el operador, con base en la información aportada por la fuente, conforme se establece en el procedimiento para consultas, reclamos y peticiones; y (iii) Solicitar prueba de la autorización, cuando dicha autorización sea requerida conforme lo previsto en la presente ley.

La Ley de Habeas Data financiera de 2008, retomó en su integridad las anteriores conceptualizaciones de fuente de información, fuente-operador, así como lo referente a los derechos del titular de los datos frente a las fuentes de información o los fuente-operadores (artículo 3º, literal b), y c), y artículo 6º, numeral 2º).

En el artículo 8º de la Ley citada, el legislador de 2008, estableció los deberes de las fuentes de información de la siguiente manera: 1. Garantizar que la información que se suministre a los operadores de los bancos de datos o a los usuarios sea veraz, completa, exacta, actualizada y comprobable; 2. Reportar, de forma periódica y oportuna al operador, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a este se mantenga actualizada; 3. Rectificar la información cuando sea incorrecta e informar lo pertinente a los operadores; 4. Diseñar e implementar mecanismos eficaces para reportar oportunamente la información al operador; 5. Solicitar, cuando sea del caso, y conservar copia o evidencia de la respectiva autorización otorgada por los titulares de la información, y asegurarse de no suministrar a los operadores ningún dato cuyo suministro no esté previamente autorizado, cuando dicha autorización sea necesaria, de conformidad con lo previsto en la presente ley; 6. Certificar, semestralmente al operador, que la información suministrada cuenta con la autorización de conformidad con lo previsto en la presente ley; 7. Resolver los reclamos y peticiones del titular en la forma en que se regula en la presente ley; 8. Informar al operador que determinada información se encuentra en discusión por parte de su titular, cuando se haya presentado la solicitud de rectificación o actualización de la misma, con el fin de que el operador incluya en el banco de datos una mención en ese sentido hasta que se haya finalizado dicho trámite; 9. Cumplir con las instrucciones que imparta la autoridad de control en relación con el cumplimiento de la presente ley; y, 10. Los demás que se deriven de la Constitución o de la presente ley.

3.1.2.2. Las Agencias de Información Comercial. Excepciones normativas.

En el literal i) del artículo 3º del proyecto de ley Estatutaria colombiana de 2006-2007, define a la “*Agencia de Información Comercial*” como “*toda empresa legalmente constituida que tenga como actividad principal la recolección, validación y procesamiento de información comercial sobre las empresas y comerciantes específicamente solicitadas por sus clientes, entendiéndose por información comercial aquella información histórica y actual relativa a la situación financiera, patrimonial, de mercado, administrativa, operativa, sobre el cumplimiento de obligaciones y demás información relevante para analizar la situación integral de una empresa. Para los efectos de la presente ley, las agencias de información comercial son operadores de información y fuentes de información*”.

En el párrafo de la norma citada, el proyecto de ley, aclara que a las agencias de información comercial, así como a sus fuentes o usuarios no se les aplicará, lo siguiente: 1. Los deberes que tienen las fuentes de la información, siguientes: ((i) Reportar, de forma periódica y oportuna al operador, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a este se mantenga actualizada; y (ii) Informar al operador que determinada información se encuentra en discusión por parte de su titular, cuando se haya presentado la solicitud de rectificación o actualización de la misma, con el fin de que el operador incluya en el banco de datos una mención en ese sentido hasta que se haya finalizado dicho trámite. 2. Lo relativo a la permanencia de la información, previsto en el artículo 13 del proyecto de ley; y 3. Lo referente al acceso a la información por parte de los usuarios, establecido en el artículo 15 del proyecto de ley.

La Ley de Habeas Data financiera de 2008, retomó en su integridad tanto la conceptualización de Agencia de información comercial, como las excepciones aplicadas a éstos operadores y fuentes de información financiera. Así quedó previsto en el artículo 3º, literal i), y en el párrafo correspondiente. El artículo 3º, literal i), fue declarado exequible por la Corte Constitucional en la Sentencia C-1011-2008, artículo 2º.

3.1.3. Los Usuarios de la información. En particular, los “usuario-fuente”.

La LPDA de 2000, define al usuario de la información, como la *“persona, pública o privada que realice a su arbitrio el tratamiento de datos, ya sea en archivos, registros o bancos de datos propios o a través de conexión con los mismos”*.

La Directiva Comunitaria No. 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, entre las definiciones que incluye no regula al usuario de la información, sino a los “destinatarios” de la misma, porque entiende que éste puede ser una persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que reciba “comunicación de datos”, se trate o no de un tercero. Aclara la directiva, que las autoridades que reciban una comunicación de datos en el marco de una investigación específica no serán considerados destinatarios ^[91].

En el proyecto de ley estatutaria colombiano No. 064 de 2003, en el extenso catálogo de definiciones, sostiene que el “usuario o destinatario” de la información, es *“toda persona a quien se suministra la información contenida en un banco de datos o central de información, debidamente autorizada por el titular”*.

Por su parte el proyecto de ley estatutaria colombiano de 2006-2007, sostiene que “usuario”, sin más, es *“la persona natural o jurídica que, en los términos y circunstancias previstos en la presente ley, puede acceder a información personal de uno o varios titulares de la información suministrada por el operador o por la fuente, o directamente por el titular de la información. El usuario, en cuanto tiene acceso a información personal de terceros, se sujeta al cumplimiento de los deberes y responsabilidades previstos para garantizar la protección de los derechos del titular de los datos. En el caso en que el usuario a su vez entregue la información directamente a un operador, aquella tendrá la doble condición de usuario y fuente, y asumirá los deberes y responsabilidades de ambos”*.

(91) En: <http://www.cc.cec>.

En el fondo esta definición de usuario se apega al texto concreto y explicativo que traía la Directiva Comunitaria europea sobre los destinatarios de la información, el cual tenía derecho a la fase de comunicación de los datos, es decir, al acceso de la información. Sin embargo, el proyecto establece una connotación especial y por su puesto un régimen igualmente especial para los que denomina “usuario-fuente”.

El proyecto de ley, regula con los derechos que tiene el titular de los datos frente a los usuarios de la información en general así: (i) Solicitar información sobre la utilización que el usuario le está dando a la información, cuando dicha información no hubiere sido suministrada por el operador; y (ii) Solicitar prueba de la autorización, cuando ella sea requerida conforme lo previsto en proyecto de ley.

Además los titulares de información financiera y crediticia, tendrán los siguientes derechos frente a los usuarios de la información: (i) Podrán acudir ante la autoridad de vigilancia para presentar quejas contra las fuentes, operadores o usuarios por violación de las normas sobre administración de la información financiera y crediticia; y, (ii) pueden acudir ante la autoridad de vigilancia para pretender que se ordene a un operador o fuente la corrección o actualización de sus datos personales, cuando ello sea procedente conforme lo establecido en la presente ley.

La Ley de Habeas Data de 2008, retoma en su integridad los conceptos de usuario, como sobre los derechos de aquél, previstos en los proyectos de ley Estatutaria, especialmente el de 2006-2007. El artículo 3º , literal d) que conceptualiza al usuario, fue declarado exequible mediante la Sentencia C-1011-2008, artículo 2º .

Por su parte el artículo 9º de la citada ley, expone los deberes que tienen los usuarios frente a los datos, el procesamiento, la consulta o la transmisión de datos. Estos son: 1. Guardar reserva sobre la información que les sea suministrada por los operadores de los bancos de datos, por las fuentes o los titulares de la información y utilizar la información únicamente para los fines para los que le fue entregada, en los términos de la presente ley; 2. Informar a los titulares, a su solicitud, sobre la utilización que le está dando a la información; 3. Conservar con las debidas seguridades la información recibida para impedir su deterioro, pérdida, alteración, uso no autorizado o fraudulento; 4. Cumplir con las instrucciones que imparta la autoridad de control, en relación con el cumplimiento de la presente ley; y, 5. Los demás que se deriven de la Constitución o de la presente ley.

3.2. Elementos materiales

3.2.1. Los datos o informaciones personales

3.2.1.1. En el ámbito comunitario europeo: Dato personal y categoría de datos.

Los datos de carácter personal o simplemente datos personales, en las normas de protección de datos personales de Europa y en particular en la Ley Orgánica de Protección de Datos Personales –LOPD– de 1999 de España, se considera como *“cualquier información concerniente a personas físicas identificadas o identificables”*. La Directiva Comunitaria 95/45/CE, adiciona a la definición anterior, *“se considera identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios específicos, características de su identidad física, fisiológica, psíquica, cultural o social”*. Sin embargo, la Directiva comunitaria inicia diciendo que datos personales es “toda información” y no “cualquier información” como lo prevé el artículo 3-a de la LOPDP española. En este mismo sentido se pronunciaba el Convenio de Estrasburgo de 1981.

Los *datos de carácter particular o datos personales*, (se excluyen los datos de las personas jurídicas, al menos del ámbito jurídico comunitario y español ^[92]), para designar a toda clase de información (textual, auditiva, de imágenes, video auditivas ^[93]) relativa a las personas naturales o físicas (identificada o identificable) o *concernidas* que son objeto de recolección, registro, tratamiento, almacenamiento y trasmisión (cesión, consulta y flujo transfronterizo de datos) por medios informáticos, electrónicos o telemáticos o no y cuya conceptualización, principios que los gobiernan, clasificación o categorización, mecanismos y procedimientos jurídicos que sirven para su tutela en vía administrativa, contencioso-administrativa y jurisdiccional (constitucional y penal, básicamente), se hallan previstos en el ordenamiento jurídico vigente español.

Sin embargo, se ha creído que el término “*cualquier información*” utilizado por la LOPDP, constituye un error de definición consistente en no haber excluido de su ámbito objetivo a un núcleo mínimo de datos, para así evitar que toda información relativa a una persona física, por nimia que parezca, constituya un dato de carácter personal a los efectos legales^[94]. Pero lo que no se repara es que la información de carácter personal a la que hace referencia la LOPDP, es la referida al concernido dentro de un marco constitucional de derechos y libertades inherentes a la persona humana (arts. 14,15, 16 y 55.1 Constitución de España o CE), valores y principios como la dignidad de la persona, el desarrollo de la personalidad, el interés público, la paz social y democrática (art. 10 CE); y los límites constitucionales a los derechos de los demás previstos en la propia CE

-
- (92) Como también lo reconoce el profesor Orti Vallejo, el art. 1 de la LORTAD, siguiendo el criterio dominante --aunque no unívoco-- de las leyes de protección de datos extranjeros (EE.UU, Alemania, Francia), deja fuera del marco protector de la misma los datos relativos a las personas jurídicas. Sin embargo, esto no implica que las personas jurídicas queden desprotegidas, pues el “prestigio o el secreto de los datos de las personas jurídicas constitucionalmente”, están cubiertos con garantías civiles como la del art. 1092 C del Comercio, entre otras posibilidades, como las garantías de protección de carácter penal. Véase, ORTI VALLEJO, Antonio. ***Derecho a la Intimidad e Informática. (Tutela de la persona por el uso de ficheros y tratamientos informáticos de datos personales. Particular atención a los ficheros de titularidad privada)***. Ed. Comares, Peligros (Granada), Esp., 1994, pág. 74 a 79
- (93) Si bien la Ley Orgánica no aludía en concreto a dichos conceptos, sí se aludía a los mismos en el art. 1-4 del Reglamento de la Agencia de Protección de Datos Española (D.R.1332/1994, de 20 de Junio), sobre información fotográfica, acústica o de cualquier otro tipo. La Directiva Comunitaria amplía el concepto de dato personal e incluye la imagen al no sólo la captada por aparato fotográfico, sino también por videocámaras y, en definitiva, por lo que puede definirse como sector audiovisual (agregaríamos con medios informáticos, electrónicos o telemáticos que manejan el dato personal de imagen). “No cabe duda que la utilización de imagen y sonido ha experimentado un gran aumento: controles de acceso a edificios, fichero de policía, utilización de la voz en el automóvil o de la imagen en controles de acceso en autopistas, en detección de infracciones de tránsito, en los servicios y comercio mediante los terminales de información, en el mundo del trabajo y de las relaciones profesionales, en el ámbito del hogar o en el terreno de la salud. El reconocimiento de la voz y el sonido como datos personales efectuado por la Directiva va a potenciar la protección de los mismos en aras de la salvaguarda de la intimidad personal (o mejor al conjunto de derechos y libertades fundamentales previstos en la CE, en el ámbito español)... “DUMORTIER, J., y ALONSO BLAS, Diana M. ***La Transposición de la Directiva de protección de datos en Bélgica***. En: Actualidad Informática Aranzadi. Ed. Aranzadi, S.A., Núm. 20 de Julio, Pamplona, 1997, pág. 5
- (94) Esto nos conduce a pensar que una “simple agenda informática de teléfonos es un fichero de datos de carácter personal, que debe ser notificado a la APD (se refiere a la “Agencia de Protección de Datos Española”) antes de su uso, a cuyo fichero hay que dotar de sistemas de seguridad adecuados, con la obligación de informar al afectado de que integramos su teléfono a un fichero automatizado, etc., “En otro lugar, con igual intención alude: “Debemos recabar un consentimiento escrito de nuestros clientes si precisamos tener datos sobre su ideología o creencias, salud o cuestiones relativas a la vida sexual, lo cual no es inusitado en nuestra profesión, en particular por parte de los abogados matrimonialistas o penalistas (art.7, núm. 2 y 3)”. Cfr. JIMENEZ ESCOBAR, Raúl. ***Sobre la aplicación de la Ley orgánica 5 de 1992 a los ficheros automatizados de datos de carácter personal mantenidos por los abogados***. En: Revista Jurídica de Cataluña No. 1, Barcelona, 1995, pág. 37 y 43

(art. 18.4., 20.1.d) y la ley (LOPD y normas de desarrollo).

En los principios relativos a la legitimación del tratamiento de datos, establece unos derechos-deberes para los titulares de los datos, así como una serie de garantías para los Estados miembros que deben implementar cuando un dato personal se someta a procedimiento informatizado. El titular de los datos o "interesado" como le llama la Directiva Comunitaria, permitirá el tratamiento informatizado de datos personales, siempre que: a) haya dado su consentimiento de forma inequívoca; b) sea necesario para la ejecución de un contrato en el que el interesado sea parte o para la aplicación de medidas precontractuales adoptadas a petición del interesado; c) sea necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento; d) sea necesario para proteger el interés vital del interesado; e) sea necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos; y, f) sea necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieren protección, en particular el derecho a la intimidad (Artículo 1-1, Directiva Comunitaria).

El Presidente del Tribunal Europeo de Derechos humanos en el discurso de apertura de la XIII Conferencia de Comisarios de protección de dato, manifestó: "*aunque hablamos de protección de datos, de legislación de protección de datos y de autoridades de protección de datos, no deben existir dudas respecto de la verdadera naturaleza del objetivo que motiva la creación de las normas de protección de datos o de las instituciones que garantizan el cumplimiento de las mismas. Su finalidad real no es tanto la protección de datos sino la protección de la vida privada de las personas en una nueva era que impone la recogida y almacenamiento de más y más datos sobre sus vidas privadas y hace aumentar la posibilidad de manipulación y mal uso de tales datos*" ^[95].

Con estos planteamientos se confirma que en el ámbito comunitario europeo, las leyes de protección de datos tienen como bien jurídico tutelado al derecho a la intimidad prioritariamente y como la información o datos del concernido son los que se pregonan de la persona física o natural.

La *Act Privacy* canadiense ^[96], yendo más allá de la enunciación abierta de "cualquier información" de la persona, para determinar qué se debe entender por dato o información personal, prefirió utilizar la fórmula o listado referencial "*The personal information*", el cual describe la información concerniente a una persona, cualquiera sean los mecanismos o tecnologías por las que se obtengan o graben. Estas son:

1) La información relacionada con la raza, origen nacional o étnico, color, religión, edad o estado civil de la persona; 2) la información relacionada con la educación, el historial médico, delictivo, laboral de la persona, o la información relacionada a las transacciones financieras en las que el individuo ha estado involucrado; 3) cualquier número o símbolo que identifique o se le asigne a una persona; 4) la dirección, las huellas digitales o el tipo sanguíneo de la persona; 5) las opiniones o ideas personales, excepto aquellas verdaderas

(95) RYSDALL, R. *Protección de datos y el Convenio Europeo de los derechos humanos*. Novática, Marzo de 1992. Citado por AA.VV. *Revista de Ciencias Jurídicas*, Facultad de derecho, Universidad de Costa Rica, No. 103, Costa Rica, 2003, p.154.

(96) AA.VV. *Banco de Datos. Biblioteca Virtual de la Universidad de Montreal Canadá (versión en inglés y en francés)*. En: www.umontreal.edu.ca

sobre otra persona, o sobre una propuesta de subvención, recompensa o un premio otorgado por una institución gubernamental, sección, departamento o Ministerio, según lo estipulen sus reglamentos; 6) la correspondencia enviada a una institución gubernamental por una persona que es implícita o explícitamente de naturaleza privada o confidencial, así como las contestaciones a la misma en la medida que revelen un contenido que corresponda a la envida originalmente; 7) las ideas u opiniones de otra persona sobre él; 8) las ideas u opiniones de otra persona sobre una propuesta de subvención, recompensa o premio otorgado por una institución gubernamental, sección, departamento o Ministerio, según lo estipulen sus reglamentos y referida en el párrafo (e), pero excluyendo el nombre de la otra persona sobre la cual dedicó sus ideas u opiniones; 9) el nombre de la persona que aparece relacionada con otra información personal y que el sólo descubrimiento del verdadero nombre revelaría información sobre aquél; pero para los propósitos de artículos 7, 8 y 26 de ésta ley y el artículo 19 de la LAIC (Ley de acceso a la información canadiense. *Access to information Act*, la información personal queda excluida. 10) la información de una persona que fue o es funcionario o empleado de una institución gubernamental y relacionada con la posición o funciones del mismo. Esta última información incluye: (i) el hecho de que el individuo es o era funcionario o empleado de la institución gubernamental; (ii) el título, dirección comercial y número del teléfono de la persona; (iii) la clasificación, rango y monto del sueldo y atribuciones según su cargo; (iv) el nombre de la persona que figura en un documento preparado por éste en el ejercicio de su empleo; y, (v) las ideas u opiniones personales expresadas en el curso de su empleo; 11) la información sobre una persona que desempeña o desempeñó los servicios bajo contrato con una institución gubernamental. Esta información incluye: los términos del contrato, el nombre del individuo y las opiniones o ideas expresadas en el transcurso del mismo; 12) información relacionada con cualquier beneficio discrecional de *naturaleza financiera*, incluida la concesión de una licencia o permiso, así como nominación del mismo, el nombre de quien la confirió y la naturaleza precisa.

La regla general para la protección de *toda información personal* en el derecho canadiense es el no descubrimiento o divulgación de los datos o las informaciones de carácter personal cuando no haya consentimiento de una persona a quien concierne una información catalogada de personal (art.3, b,) y siempre que ésta se halle bajo el control o responsabilidad de una institución gubernamental. La excepción, es que se podrá descubrir la información, previos un procedimiento administrativo breve y sumario en las doce situaciones previstas en el art.8.2. de la *Act Privacy* [Mackenzie vs. Canadá (Ministerio de Salud Nacional y Bienestar Social). 1994. Primera Instancia. Corte Federal Canadiense F.C.TD.]. Estas que se pueden catalogar de excepciones al descubrimiento o divulgación de la información por parte de un organismo del Estado, tienen como fundamento la realización de algunos de los fines de un Estado de derecho, tales como la seguridad, la defensa, la salubridad y la economía públicas, o bien los intereses generales, públicos, de relaciones internacionales, investigativos (judiciales o administrativos), científicos o archivísticos o, en últimas, los del concernido o interesado con la información ^[97].

Por el contrario en el derecho europeo, respecto de los datos que la doctrina mundial llama "*datos sensibles*" de la persona humana, que afectan el "*núcleo duro de la privacy*" o la intimidad ^[98], la Directiva Comunitaria 95/46/CE, prefirió establecer unas "categorías

(97) RIASCOS GOMEZ, Libardo O. *Los datos personales informatizados en el derecho foráneo y colombiano*. Evaluada por la Universidad Nacional, UDENAR, Pasto, 2002, p. 47 y ss.

(98) Ob., ut supra cit.

especiales de tratamientos”, a fin de que los Estados Miembros de la CE al transponer la normatividad a su derecho interno, observaran los lineamientos o directrices planteados en la Sección III, artículo 8, que es del siguiente tenor:

Los Estados Miembros prohibirán el tratamiento de datos personales que revelen el origen Racial o étnico, las opiniones públicas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad.

Esta regla general, tiene una serie de excepciones, restricciones y limitaciones tanto comunitarias como para ser aumentadas o moduladas por los diferentes Estados miembros de la UE. Entre las excepciones, a la regla están: (i) Cuando el interesado haya dado su consentimiento explícito a dicho tratamiento, salvo en los casos en los que la legislación del Estado miembro disponga que la prohibición establecida, no pueda levantarse con el consentimiento del interesado; (ii) Cuando el tratamiento sea necesario para respetar las obligaciones y derechos específicos del responsable del tratamiento en materia de derecho laboral en la medida que esté autorizado por la legislación y éste prevea garantías adecuadas; (iii) Cuando el tratamiento sea necesario para salvaguardar el interés vital del interesado o de otra persona, en el supuesto de que el interesado esté física o jurídicamente incapacitado para dar su consentimiento; (iv) Cuando el tratamiento sea efectuado en el curso de sus actividades legítimas y con las debidas garantías para una función, una asociación o cualquier otro organismo sin fin de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refiera exclusivamente a sus miembros o a las personas que mantengan contactos regulares con la fundación, la asociación o el organismo por razón de su finalidad y con tal de que los datos no se comuniquen a terceros sin el consentimiento del interesado; y (v) Cuando el tratamiento se refiera a datos que el interesado haya hecho manifiestamente públicos o sea necesario para el reconocimiento, ejercicio o defensa de un derecho en procedimiento judicial

La Directiva hace énfasis en las excepciones relativas al derecho a la salud de la personas; sobre infracciones, condenas penales o medidas de seguridad, y sobre el número de identificación de las personas, así: (i) Cuando el tratamiento de datos resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamiento médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos sea realizado por un profesional sanitario sujeto al secreto profesional sea en virtud de la legislación nacional, o de las normas establecidas por las autoridades nacionales competentes, o por otra persona sujeta asimismo a una obligación equivalente al secreto; y (ii) El tratamiento de datos relativos a infracciones, condenas penales o medidas de seguridad, sólo podrá efectuarse bajo el control de la autoridad pública o disposiciones nacionales que prevean garantías apropiadas y específicas. Sin embargo, sólo podrá llevarse un registro completo de condenas penales bajo el control de los poderes públicos; y (iii) Los Estados miembros determinarán las condiciones en las que un número de identificación o cualquier otro medio de identificación de carácter general podrá ser objeto de tratamiento.

Por su parte, la Ley Orgánica de protección de datos de España, en el artículo 7º a 12º, al transponer la normatividad comunitaria al derecho interno español, dispone sobre los que llama “Datos especialmente protegidos”, las siguientes reglas y excepciones: 1. De acuerdo con lo establecido en el apartado 2 del artículo 16 de la Constitución, nadie podrá ser obligado a declarar sobre su ideología, religión o creencias.

Cuando en relación con estos datos se proceda a recabar el consentimiento a que se refie

re el apartado siguiente, se advertirá al interesado acerca de su derecho a no prestarlo.

2. Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado.

3. Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una Ley o el afectado consienta expresamente.

4. Quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual.

5. Los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las Administraciones Públicas competentes en los supuestos previstos en las respectivas normas reguladoras.

6. No obstante lo dispuesto en los apartados anteriores podrán ser objeto de tratamiento los datos de carácter personal a que se refieren los apartados 2 y 3, cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto.

También podrán ser objeto de tratamiento los datos a que se refiere el párrafo anterior cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento.

Así mismo, establece una protección adicional a los tratamientos de datos relativos a la salud por normas nacionales y autonómicas; aplicar medidas de seguridad máximas (técnicas y organizativas) a los datos anteriormente relacionados; potenciar el deber de secreto o sigilo profesional en los datos que proceda; regular en forma especial en la fase de comunicación de datos, la regla general y las excepciones al consentimiento del “afectado o interesado” con el tratamiento de datos; y regular con suma cuidado el acceso a los datos por cuenta de terceros ^[99].

(99) El Artículo 12 de la LOPD de España, al respecto dispone: Acceso a los datos por cuenta de terceros.1. No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento. 2. La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas. En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar. 3. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento. 4. En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado, también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

3.2.1.2. En el ámbito Latinoamericano: Datos o Informaciones personales. Diversa protección según la clasificación de los datos

En el derecho latinoamericano, la definición de datos personales no solo se predica de las personas naturales sino también de las personas jurídicas. En efecto, en la LPDA de 2000, los datos personales constituyen la *“información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables”*, es decir, que incluye la información generada por las personas jurídicas, morales o de “existencia ideal”.

En casi todas las leyes de protección de datos (Argentina), de protección a la vida privada (Chile), de acceso a la información pública y de transparencia de la gestión pública (Honduras), de protección al dato financiero (Uruguay); entre otras, contienen definiciones sobre los datos o informaciones personales, similares a las que trae la LPDA de 2000, la cual a su vez, retoma la definición y los parámetros conceptuales del derecho europeo. Por eso con la definición de la LOPD es prototípica.

Así mismo, la LPDA clasifica a los datos personales generales o simplemente “datos personales” y a los “datos sensibles” o pertenecientes al núcleo duro de la intimidad. Estos últimos se definen como aquellos *“datos personales que revelan origen racial o étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual”*.

En idéntico sentido regula la definición de datos sensibles la Ley Chilena No. 19.628 de 28 de Agosto de 1998, “sobre protección a la vida privada o protección de los datos de carácter personal” y la Ley No. 17938 de Octubre 1º de 2004 o *“Ley de protección de datos personales para ser utilizados en informes comerciales y el Hábeas Data”* del Uruguay (LPDP_HDU).

En el derecho colombiano, en los primeros proyectos de leyes estatutarias del Hábeas Data Integral, general o en la mayor de las veces de carácter sectorial (hacia el dato financiero), posterior a 1995, se ha incluido en el capítulo definiciones las atinentes a los datos personales y los datos sensibles, siguiendo los cuadros normativos latinoamericanos, ya que en el derecho continental europeo, los “datos sensibles” son una categoría de datos surgida en los tratados o estudios doctrinarios de los juristas, más que en la plasmación de textos normativos, como hemos visto. A partir de 2002 y hasta Junio de 2007 en los proyectos de ley estatutaria, además de las definiciones de datos personales y datos sensibles se aumentaron otras tales como: dato negativo, dato público, dato privado y dato semi-privado que más adelante precisaremos.

Así por ejemplo, en el Proyecto de Ley estatutaria acumulado 201 de Cámara, 071 de 2002 de Senado, relativo a *“Por la cual se regula integralmente el derecho fundamental al habeas data y demás libertades y derechos fundamentales de las personas en lo que respecta al tratamiento de sus datos personales a través de bases de datos públicas y privadas, y se dictan otras disposiciones”*^[100], los ponentes introducen una definición de dato personal, ampliada a la del derecho europeo y el latinoamericano, al afirmar que éste es

(100) El intitulado del proyecto original era: “por la cual se regula el derecho de acceso a la información de interés público, en particular la de carácter comercial, financiero, la que tiene que ver con el cumplimiento de obligaciones fiscales y parafiscales y con el pago de servicios públicos domiciliarios, y se dictan otras disposiciones”. Vid. HERNANDEZ, Jaime A. y VARGAS, Javier. **Pliego de modificaciones al proyecto de ley Estatutaria 201 de 2003 y 071 de 2002 Senado**. Ponentes del proyecto acumulado. Vía Internet.

“toda información relativa a personas físicas, jurídicas o de hecho que de cualquier manera sea idónea para permitir, directa o indirectamente, su identificación tales como, entre otros, los nombres y apellidos, los números de identificación personal, los datos financieros, tributarios o de solvencia patrimonial o crediticia”. Se amplía en la cobertura de aplicación de la definición, pues se entiende a las “personas de hecho” y se incluye aspectos de identificación de las personas humanas y jurídicas, tanto de derecho público como de derecho privado.

También por inclusión de los ponentes, se define al “dato sensible”, como *“aquel dato personal cuyo contenido involucra riesgos de prácticas discriminatorias por razones raciales y étnicas, opiniones políticas, convicciones religiosas, filosóficas o morales, la afiliación sindical, informaciones relacionadas con la salud, la vida sexual o cualquier otra circunstancia similar de carácter personal o social”*. Y agrega en el inciso 2º: *“La recolección, almacenamiento, procesamiento, tratamiento, uso y suministro del dato sensible requerirá del consentimiento expreso, previo y escrito de su titular”*.

El dato o “información sensible” como prefiere denominarla el proyecto, le asigna un plus de protección frente a los demás datos o informaciones personales. Este plus de protección está previsto en los artículos 4º y 27º así: (i) Se requiere el consentimiento, previo y escrito del titular del dato, si por excepción es sometido a tratamiento o procesamiento de datos; (ii) Nadie está obligado a proporcionar datos sensibles; (iii) Sin consentimiento pueden ser sometidos a tratamiento de datos, “cuando medien razones de interés general autorizados por ley” o cuando se persiga “finalidades estadísticas o científicas” y “no puedan ser identificados sus titulares”; y, (iii) Queda prohibida la formación de archivos, bancos o registros que almacenen información que directa o indirectamente revelen la identidad del titular de los datos sensibles. Sin perjuicio de ello, las iglesias, las asociaciones religiosas y las organizaciones políticas y sindicales podrán llevar un registro de sus miembros.

Por su parte, el proyecto de ley estatutaria del Hábeas Data No. 064 de 2003, a instancia de la Defensoría del Pueblo, en el artículo 5º, amplía aún más la definición del anterior proyecto, al sostener que “dato personal” es *“toda información relativa a personas físicas, jurídicas o de hecho que de cualquier manera sea idónea para permitir, directa o indirectamente, su identificación, tal como el nombre y apellidos, número de identificación personal, voz e imagen, o datos financieros, tributarios o de solvencia patrimonial y crediticia”*. La amplia en los identificadores de las personas físicas o naturales: voz e imagen; y mantiene en los de las personas jurídicas y de hecho.

En cuanto, al “dato sensible”, en el numeral 7 del artículo citado, lo define como *“aquel dato referido al origen racial o étnico, las opiniones políticas o filosóficas, las convicciones religiosas, la pertenencia a sindicatos o relativos a la salud o la sexualidad de una persona, cuyo tratamiento está proscrito por involucrar riesgo de prácticas discriminatorias”*. En esencia esta se mantiene la definición del proyecto anterior, pero se mejora en la redacción de la norma. El inciso 2º mantiene la esencia del consentimiento del titular con el nombre de autorización del titular de los datos, al decir: *“La recolección, registro, almacenamiento, procesamiento, tratamiento, uso y suministro del dato sensible sólo se hará en los casos y para los fines previstos en esta ley”*.

El dato sensible sigue siendo ultra protegido en todas las fases del tratamiento o procesamiento de datos personales, al punto que esta práctica se prohíbe por regla general (artículo 34) y solo por excepción se permite cuando el titular de los mismos otorga *“autorización (previa y escrita) sólo para el tratamiento con fines históricos, científicos, estadísticos u otros de interés general previstos de forma expresa en la ley”*. Se refuerza, cuando dice: *“ninguna persona está obligada a proporcionar datos sensibles”* (artículo 67),

salvo que “*medién razones de interés general autorizadas por la ley*” o para los fines anteriormente relacionados.

En el proyecto de Ley Estatutaria del Hábeas Data No. 071 de Cámara de 2005, que quizá sea uno de los más prolíficos en definiciones que se haya presentado al Congreso de la República, no solo suministra definiciones técnico-jurídicas aplicables al Hábeas Data, sino que las clasifica. Así dentro de las definiciones en “relación a la clasificación de los datos según su naturaleza” incluye: el dato personal, el dato público, el dato privado, el dato semi-privado y el dato íntimo, y en “otras clasificaciones”: “dato” y “registro individual.

Define como “*dato personal...cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica. Los datos impersonales no se sujetan al régimen de protección de datos de la presente ley. Cuando en la presente ley se haga referencia a un dato, se presume que se trata de uno personal. Los datos personales pueden ser públicos, semiprivados o privados*”.

De esta definición se infiere las suministradas por separado como “dato” y “registro individual”, por lo cual se consideran innecesarias tales definiciones ^[101]. Ahora bien, se maneja una definición amplísima de dato personal cuando se hace referencia a “cualquier pieza de información”, aún cuando luego se refiera a la presunción que puede ser desvirtuada de dato solo referido a lo personal, pues si lo que se quería expresar es que la información, como se sostuvo anteriormente se concreta desde una manifestación informática binaria hasta un dato escrito o electrónico, auditivo, visual, audiovisual o telemático, estos no son “piezas” sino medios de crear, conseguir o recuperar información. Hoy conocemos medios escritos o tradicionales y medios electrónicos, telemáticos o informáticos ^[102]. En tal virtud, es universalmente entendible la definición que inicie sosteniendo “*cualquier información...*” referida a la persona física o jurídica.

El proyecto de ley, distingue entre dato sensible y dato íntimo, por vez primera para esta clase de normas, no sólo en el ámbito europeo, sino en el Latinoamericano.

En efecto, respeto al dato sensible lo define como “*aquel dato personal que puede potencialmente ser utilizado para discriminar a las personas, como es el relativo a la raza, la ideología o la orientación sexual*”. Reduce, con relación a los anteriores proyectos de ley e incluso en lo pertinente a las legislaciones europeas y latinoamericanas, de una forma significativa el contenido del concepto de dato sensible a tres aspectos que pueden

(101) En el numeral 17 se manifiesta: “Dato: Es toda pieza individual de información contenida en los bancos de datos” y en el numeral 19, “Registro individual: Se refiere al conjunto de datos contenido en una base de datos relativo a un único titular de la información”.

(102) Los medios escritos, documentales o tradicionales, son todos aquellos mediante los cuales se elabora, crea, modifica, archiva, procesa o destruye todo tipo de información no solo concerniente a las personas humanas o jurídicas, sino la referente a hechos, circunstancias, eventos no personales. En cambio, los medios electrónicos, telemáticos o informáticos, son aquellos mediante los cuales se trata o procesa información electrónica, con apoyo de las nuevas tecnologías de la información y la comunicación (TIC) y a través de software (programas de computador), hardware (equipos computacionales) y diversos elementos electro-magnéticos (Discos fijos y movibles, Discos compactos: CD, DVD, DI, etc., Disquetes; entre muchos otros.). El procesamiento electrónico de datos produce documentos electrónicos (El EDI anglosajón); bancos, bases, ficheros o registros electrónicos de datos de todo tipo, incluidos los bancos de datos personales, objeto y finalidad de leyes y proyectos de ley del Hábeas Data. Vid. RIASCOS GOMEZ, Libardo O. **EL derecho a la Intimidad, la visión ius-informática y los delitos relativos a los datos personales**. Tesis Doctoral, Universidad de Lleida (España), Lleida, 1999, p. 286 y 505

discriminar a la persona: la raza, la ideología o la vida sexual.

El dato íntimo, se considera *“el dato que, por su contenido o su naturaleza, las personas habitualmente prefieren mantenerlo en reserva y su conocimiento por parte de terceros no representa un interés general legítimo, como es el referido a los hábitos personales o a la vida familiar”*. Podría decirse que estos son los datos del círculo profundo de la vida privada a los que solo llega la misma persona y no representan alguna importancia o interés sino para su titular. Pese a que puede ser asimilable teóricamente el dato íntimo, es difícil distinguirlo de un dato anodino o superfluo para las demás personas pero para su titular de gran importancia y susceptible de tutela jurídica por el Estado. Por eso decíamos *ut supra* que en un dato anodino se puede esconder un dato personal o familiar, o viceversa y en ese hilo delgado de distinción se pueden cometer serias injusticias o desprotección estatal del derecho a la intimidad, al honor, al buen nombre, a la imagen, etc.

Por esto se considera innecesaria e inconveniente la definición suministrada. Sin embargo, el proyecto de ley para definir “el dato privado” toma como base las definiciones de dato sensible y dato íntimo. Sobre este aspecto más adelante profundizaremos.

Finalmente, el proyecto de ley estatutaria No. 221/2007 de Cámara y No. 027/2006 de Senado, acumulado con el No. 05/2006 Senado, “Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial y de servicios y se dictan otras disposiciones”, en el artículo 3º relaciona unas definiciones técnico-jurídicas aplicables al tratamiento o procesamiento de datos personales informatizados o no y en particular a las facultades o componentes del Hábeas Data, con énfasis financiero.

Este proyecto al igual que los anteriores prosigue con la distinción entre dato personal, dato público, dato semi-privado y privado, elimina la definición de dato íntimo y agrega la que llama *“Información financiera, crediticia, comercial, de servicios y la proveniente de terceros países”*. Concordantemente con esto último, el catalogo de definiciones comienza con explicar qué debe entenderse por “titular de la información, y al efecto, dice: *“Es la persona natural o jurídica a quien se refiere la información que reposa en un banco de datos y sujeto del derecho de hábeas data y demás derechos y garantías a que se refiere la presente ley”*.

El dato personal, según el literal e, del artículo 3º del proyecto, es *“cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica. Los datos impersonales no se sujetan al régimen de protección de datos de la presente ley. Cuando en la presente ley se haga referencia a un dato, se presume que se trata de uso personal. Los datos personales pueden ser públicos, semi-privados o privados”*.

La presente definición se mantienen los elementos suministrados en el proyecto 071 de 2005 y por tanto, son válidas para ésta las observaciones anteriormente realizada para éste proyecto.

Sobra haberse reiterado en la definición que no tienen sujeción al régimen jurídico del presente proyecto de ley estatutaria, los datos impersonales o no atribuibles a una persona determinada, o según el diccionario que *“no se aplica a nadie en particular”*, pues según el intitulado y en el contexto del proyecto la ley se dice que rige para los datos personales o de la persona física o jurídica determinada o determinable. Estos datos

impersonales tal como están excluidos de regulación podrían confundirse con los datos personales que han sido sometidos a procedimiento de disociación de manera que la información que se obtiene no puede asociarse a una persona determinada o determinable. Estos datos disociados son objeto de regulación por parte de la LOPDP española de 1999, los datos disociados a efectos de la comunicación (circulación, transferencia o cesión) de los datos son perfectamente posible sin necesidad de consentimiento y sin la previsión de derechos de cedente y cesionario (artículo 11º).

Por otra parte, parecería que no es dato personal la “*Información financiera, crediticia, comercial, de servicios y la proveniente de terceros países*”, que el proyecto de ley define en el literal j), del artículo 3º. Parecería decimos, porque a renglón seguido de definir el dato personal dice que “*pueden ser públicos, semi-privados o privados*” y excluye a propósito la información o datos financieros. Sin embargo, al emplear el término “pueden” se entiende que además de los mencionados en dicha definición caben otras posibilidades como la que mencionamos. Esto es de capital importancia para el proyecto de ley de Hábeas data sectorial, pues éste hace énfasis en el dato financiero.

Esta subespecie de dato personal se define así: “*información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, aquella referida al nacimiento, ejecución y extinción de obligaciones dinerarias, independientemente de la naturaleza del contrato que les dé origen, **así como la información relativa a las demás actividades propias del sector financiero o sobre el manejo financiero o los estados financieros del titular***” (Declarada inexecutable mediante la Sentencia C-1011-2008) ^[103].

Esta definición de dato personal de carácter financiero, con algunos leves retoques y salvo la frase declarada inexecutable quedó plasmado en la Ley de 2008, en el artículo 3º, literal j), de la siguiente manera: “*Información financiera, crediticia, comercial, de servicios y la proveniente de terceros países. Para todos los efectos de la presente ley se entenderá por información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, aquella referida al nacimiento, ejecución y extinción de obligaciones dinerarias, independientemente de la naturaleza del contrato que les dé origen*”.

El legislador de 2008, hizo énfasis en esta conceptualización, porque al fin de cuentas, la Ley de Habeas Data financiero, descansa todo su peso conceptual y legislativo en dicho concepto.

En cuanto a las conceptualizaciones sobre dato personal y demás clasificaciones sobre los datos (público, privado y semi-privado), la Ley de Habeas Data, retomó en su integridad las que finalmente dejaron los proyectos acumulados de Ley Estatutaria de 2006-2007, puesto que fueron eliminados conceptos básicos para una legislación integral de Habeas Data, tales como los “*Datos Sensibles*”, excluidos de todo sistema de procesamiento informático o en el peor de los casos, solo procesados en algunas fases

(103) La Corte Constitucional en uno de sus apartes sostiene la Inconstitucionalidad en los siguientes términos: “*El primero de los contenidos normativos expuestos, en criterio de la Sala, se muestra problemático en términos de protección del derecho fundamental al hábeas data, en especial respecto a la eficacia del principio de finalidad predicable de la administración de datos personales. En efecto, una expresión que confiera la condición de dato financiero, comercial y crediticio a todo dato relativo a las actividades financieras, resulta una cláusula en extremo genérica y vaga, por lo que impide identificar con exactitud a qué tipo de información se refiere, situación que posibilitaría la administración de datos personales que, incluso, no guarden relación con el cálculo del riesgo crediticio, en tanto finalidad constitucionalmente legítima. Bajo estas circunstancias, no existe un contexto lo suficientemente claro para el ejercicio del derecho al hábeas data en relación con esa modalidad de datos personal, lo que justifica la inconstitucionalidad del precepto*”.

del procedimiento, previo consentimiento expreso y escrito del titular y con una serie de garantías y protecciones reforzadas, como sucede en el derecho europeo continental.

3.2.2. Clases de datos o “informaciones” personales

Tradicionalmente los datos personales en el derecho continental europeo, por la naturaleza jurídica, contenido y objeto de tutela jurídica de las leyes protectoras de datos personales, sólo distinguen una clase genérica de datos, los dirigidos a la persona humana o natural y denominados “datos de carácter personal o datos personales”, pues como hemos visto anteriormente, no cabe a través de ésta clase de leyes o normas comunitarias con esas mismas finalidades (Directiva 95/46/CE y 97/66/CE), tutelar los derechos de las personas jurídicas, morales o “de existencia ideal”.

Dentro del género de los datos personales están “las categorías especiales de tratamientos” previstas en el artículo 8 de la Directiva 95/46/CE, o los “Datos especialmente protegidos”, según el artículo 7 de la Ley Orgánica de protección de datos española de 1999. Es decir, las especies de datos personales que la doctrina conoce como “datos sensibles” y los considerados ultra sensibles. Estos datos hacen referencia origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, a la salud o a la sexualidad. El primero, el segundo y el último son los datos ultra sensibles pues las normas comunitarias deprecian medios de defensa, protección y tutela jurídica efectiva mayor que el resto de datos sensibles.

En el derecho latinoamericano, las normas protectoras de datos, de la vida privada, del acceso a la información pública, mantienen la clasificación genérica del derecho europeo, pero elevan a rango legislativo lo que allá es doctrina, cuando regulan en forma expresa los datos personales sensibles, que por definición y esencia sólo pueden ser atribuibles a la persona humana o física.

En el derecho colombiano, los diferentes proyectos de ley estatutaria de Hábeas Data desde 1995 hasta Junio de 2007 como hemos visto, han regulado positivamente no sólo la categoría genérica de datos personales, atribuible a personas físicas, jurídicas y “de hecho”, sino a los datos sensibles, considerados éstos en un mismo plano de protección reforzada, pero no ultra potenciada como en el derecho europeo.

Además de éstos datos, a partir de los proyectos de ley estatutaria de Hábeas Data No. 201 de 2003 de Cámara y 071 de 2002 de Senado, se comenzó a incrementar la clasificación unas especies de datos personales, a fin de modular el grado e intensidad de protección por parte del Estado. Así se menciona el dato negativo. Luego en el Proyecto de ley No. 071 de 2005, el listado aumenta a datos públicos, datos privados, datos semi-privado y datos íntimos. Finalmente el Proyecto de Ley Estatutaria No. 221/2007 de Cámara y No. 027/2006 de Senado, acumulado con el No. 05/2006 Senado, mantiene la clasificación anterior, pero elimina la definición separada de los “datos íntimos” y la incorpora a la de los datos privados y elimina definitivamente la conceptualización de los “datos sensibles”.

Este mismo y último proceder del proyecto acumulado de 2006-2007, adoptó la Ley 1266 de 2008 en el artículo 3º, literales e), hasta el h), declarados exequibles por la Sentencia C-1011-2008, artículo 2º de la Corte Constitucional.

3.2.2.1. Dato o “información” negativa y Dato o “información” positiva

Según el proyecto de ley estatutaria de Hábeas Data No. 201 de 2003 de Cámara y 071 de 2002 de Senado, se define al dato negativo como *“todo dato cuyo tratamiento, circulación o uso legítimos puedan ocasionar perjuicios, vulneraciones o amenazas a la intimidad, libertad, identidad y buen nombre de su titular, tales como, entre otras, la que indica situaciones de incumplimiento de obligaciones de contenido económico respecto de sus titulares o los antecedentes penales”* ^[104]. En esta primera definición se entienden como datos negativos los de carácter financiero (bancario, económico, comercial, tributario, fiscal o tarifario), aunque por la utilización de los condicionantes: “tales como” o “entre otras”, se subentiende que pueden darse otras eventualidades, pero circunscritas a la regulación del proyecto de ley referido.

El proyecto de Ley estatutaria No. 064 de 2003, a iniciativa de la Defensoría del pueblo hace mención al dato negativo al hablar del deber de notificar que tienen las fuentes de información a la persona afectada con la existencia de éste, con el objeto de que ella presente las observaciones o pruebas que considere pertinentes para evitar la incorporación en la base de datos o archivo, o la circulación, de esa clase de datos. La notificación debe realizarse con anterioridad al momento en que la fuente comunique la información al banco de datos o central de información. Esta notificación hace parte del derecho fundamental al debido proceso y, en consecuencia, es indisponible e irrenunciable, según el artículo 8º numeral 13 y agrega el inciso in fine de esa norma: El titular dispone de un plazo de ocho (8) días para pronunciarse al respecto.

El dato o información positivo se hallaba inmersa en el artículo 9º de proyecto, dentro de los deberes de los operadores de los bancos de datos o de las Centrales de información, los cuales debían *“abstenerse de utilizar en los reportes que suministren a los usuarios de la información, signos o convenciones que lleven a desvirtuar la información positiva explícita o impliquen información negativa que ya ha sido desvirtuada o respecto de la cual se ha producido la caducidad”*.

En el artículo 63 del proyecto de ley, establecía rigurosamente el término de permanencia de la información contenida en los bancos de datos de solvencia patrimonial o financiera, así: 1. La información histórica negativa no podrá exceder de cinco (5) años contados a partir del momento en que se haya producido el respectivo pago como resultado de un proceso ejecutivo iniciado en contra del deudor. Eventualidades: (i) Este término se reducirá a dos (2) años cuando el pago se produzca con la sola notificación del mandamiento del pago; (ii) Si el demandado en el proceso ejecutivo invoca excepciones y éstas prosperan, y la obligación se extingue porque así lo decide la sentencia, el dato que posea el banco de datos al respecto debe desaparecer inmediatamente; 2. El término de permanencia de la información histórica negativa no podrá exceder de dos (2) años contados a partir del momento en que se haya producido el pago voluntario de la obligación pendiente; 3. El término de permanencia de la información histórica negativa en el caso del no pago de la obligación respectiva, será de cinco (5) años, a contar una vez cumplido el término de la prescripción ordinaria; 4. En el caso en que la mora en la que incurre el deudor para el pago de la obligación reportada haya sido inferior a un (1) año, el término de permanencia de la información histórica negativa no podrá exceder del doble de la misma mora; y, 5. El término de vigencia histórica de la información positiva será de cinco (5) años, al cabo de los cuales el banco de datos podrá suprimirla a solicitud del interesado.

(104) El texto en cursiva es el que incorporaron los ponentes a través del pliego de modificaciones propuesto en aquella época. Vid. HERNANDEZ, Jaime A. y VARGAS, Javier. **Pliego de modificaciones al proyecto de ley Estatutaria 201 de 2003 y 071 de 2002 Senado**. Ponentes del proyecto acumulado. Vía Internet.

En la exposición de motivos del proyecto ^[105] se explicaba este proceder, porque en la “información negativa” y la “información positiva” había que seguir los lineamientos previstos en la Sentencia SU-082 de 1995 de la Corte Constitucional, “aunque con algunas variantes”: (i) En primer lugar, se ha suprimido la circunstancia que condiciona el cumplimiento de la caducidad del dato negativo a que no ingresen nuevos datos negativos del mismo deudor, por considerar que cada obligación es autónoma, de manera que las consecuencias negativas de una obligación en mora no pueden ser trasladadas a otra; (ii) se contempla una caducidad del dato especial para el caso de la prescripción de la obligación, la cual se fija en cinco (5) años, contados a partir del término de la prescripción ordinaria (10 años); y (iii) la caducidad de la información positiva, es decir, aquella que no se refiere a incumplimiento de obligaciones o a otras circunstancias desfavorables, la cual puede ser suprimida a solicitud del titular una vez cumplida la vigencia de la misma, establecida en cinco (5) años. Esto debido a que la temporalidad de la información no se aplica sólo a los datos negativos, sino también a los positivos, siempre que el titular así lo requiera.

Por su parte, el numeral 10º del artículo 5º del proyecto de ley estatutaria de Hábeas Data preparado por la Defensoría del Pueblo en el año de 2005, en forma más amplia e integral, tal como estaba concebido todo el proyecto, definía al dato negativo, como aquel *“susceptible de tratamiento que refleja una conducta o hecho relativo al incumplimiento de los deberes u obligaciones que le son exigibles al titular de los mismos por disposición constitucional, legal, contractual o reglamentaria, o aquel que se refiere a una situación específica en la que se encuentra el titular que puede implicar una restricción, limitación o marginamiento legítimos respecto de sus derechos, garantías o expectativas de acceder a un bien o servicio”*.

Uno de los principios del tratamiento de datos previsto en este proyecto de ley y el cual tenía en cuenta la “información negativa”, era el de contradicción por el cual todo *“reporte de información negativa sobre incumplimiento de obligaciones de cualquier naturaleza, que hagan las fuentes de información a los bancos de datos o centrales de información, debe ser comunicado oportunamente al titular de los datos, con el fin de que éste pueda, si así lo decide, presentar las pruebas o argumentos enderezados a aclarar la situación”*. Esto para garantizar el derecho de defensa en diligencias o procedimientos administrativos como pudiera ser el procedimiento informático o de Hábeas Data administrativo generado por los respectivos recursos administrativos previstos en el proyecto de ley.

Además, por la regulación integral del Hábeas Data, prevista en el proyecto de ley, permitía hablar de “obligaciones de cualquier naturaleza”, y no exclusivamente las de índole financiero como había pasado en anteriores proyectos de ley. Además porque era un deber de las fuentes de información, el informar a las personas concernidas con una información negativa previstas en un reporte en el estén afectadas, *“con el objeto de que ella presente, si así lo desea, las observaciones, pruebas o comentarios que considere pertinentes. La comunicación debe realizarse en el momento en que la fuente reporte la información al banco de datos o central de información”* (numeral 5º del artículo 9º).

En el esquema de deberes y derechos, en relación a la “información positiva” y la “información negativa”, el proyecto sostenía que era deber de los responsables de los bancos de datos, *“abstenerse de utilizar en los reportes que suministren a los usuarios de*

(105) CIFUENTES MUÑOZ, Eduardo. *Exposición de motivos del proyecto de ley estatutaria No. 064 de 2003*. Vía Internet

la información, signos o convenciones que lleven a desvirtuar la información positiva explícita o impliquen información negativa que ya ha sido desvirtuada o respecto de la cual se ha producido la caducidad” (artículo 10º). Así mismo que era un derecho de los titulares de los datos, si aquello ocurriera: “Exigir la exclusión de la información negativa, de acuerdo con el plazo establecido en esta ley” (artículo 14-6).

Estaba prohibida la operación de bancos de datos que sólo traten información negativa así “La información relacionada con el incumplimiento o cumplimiento tardío de obligaciones derivadas de la prestación de servicios públicos domiciliarios o de salud o educación no será susceptible de reporte a los bancos de datos de naturaleza privada en ningún caso”(artículo 39). Sin embargo, se les permitía a “los bancos de datos de naturaleza privada procederán oficiosamente, y sin perjuicio de la facultad que asiste a los titulares de datos, a suprimir toda información negativa cuyo término de vigencia se haya cumplido al momento de entrar en vigencia la presente ley”. Y agrega el inciso 2º: “Para la depuración y actualización de los registros, los bancos de datos dispondrán de un término máximo de seis (6) meses, a partir de la vigencia de la presente ley” (artículo 52 Parágrafo transitorio).

Finalmente, sobre el “término de permanencia de los datos negativos del deudor contenida en los bancos de datos de solvencia patrimonial o financiera no podrá exceder de dos (2) años”. Y agregaba el inciso 2º: “El término de vigencia histórica de la información positiva será de cinco (5) años, al cabo de los cuales el banco de datos deberá suprimirla a solicitud del interesado”.

El Proyecto de ley estatutaria de Hábeas Data No. 071 de 2005 de iniciativa gubernamental y parlamentaria ^[106], en forma expresa no aparece la denominación de datos o informaciones negativas y/o positivas, pero sí aparece en el artículo 28, la que llama *Información desfavorable*”, a efectos de manifestar que “se prohíbe la administración de datos personales con información exclusivamente desfavorable”.

Por deducción, estimamos que el proyecto de ley se refiere en el artículo 27 a la información o datos negativos y a los positivos, al momento de hacer referencia al término de permanencia de los datos. Se infiere los datos negativos cuando “cuyo contenido haga referencia al tiempo de mora, tipo de cobro, estado de la cartera y, en general, a aquellos datos referentes a una situación de incumplimiento de obligaciones, se registrarán por un término máximo de permanencia, vencido el cual deberá ser retirada de los bancos de datos por el operador, de forma que los usuarios no puedan acceder o consultar dicha información”. Se infiere que hace mención a la información positiva, cuando se refiere al “término de permanencia de esta información será de cinco (5) años contados a partir de la fecha en que se pone al día la cuota o la obligación vencida”

En la exposición de Motivos del proyecto de ley ^[107], respecto a los datos positivos, manifestaban: “la información histórica sobre los hábitos de pago de los deudores es un activo invaluable para tener mayor acceso al crédito. Casi más importante que la información negativa (casos de mora) que reposa en estas bases de datos, es la información positiva. Pruebas documentadas sobre un comportamiento de pagos impecable en materia de impuestos, servicios públicos o préstamos, por ejemplo, puede

(106) HERNANDEZ, Jaime Amín, ARBOLEDA PALACIO, Oscar, Pérez, Oscar Darío Pérez, CARRASQUILLA, Alberto. **Proyecto de ley estatutaria No. 071 de 2005, presentado a iniciativa parlamentaria y gubernamental**. Vía Internet.

(107) Ob., ut supra cit.

constituirse en la mejor carta de presentación para un banco. Esto es particularmente importante para aquellas personas de estratos más bajos que no poseen riqueza para respaldar o garantizar un crédito y cuyo principal activo es su carácter y responsabilidad en el manejo de sus finanzas personales o microempresariales. Las bases de datos con historias crediticias de microempresas se han convertido en una fuente indispensable para las entidades que otorgan microcrédito en muchos países, y han sido un catalizador importantísimo de estas fuentes de crédito para miles de personas. Así, a través de estas centrales de información se permite a los deudores generar señales hacia el mercado que faciliten su acceso al crédito". En este sentido se ha pronunciado la Corte Constitucional en la Sentencia T-303 de 1998 se pronunció así: "Ahora bien, lo que sí puede ocurrir -y esta Corte lo ha admitido en guarda del derecho que tiene el sector financiero a estar informado oportunamente sobre los antecedentes más próximos de sus actuales o potenciales clientes y con miras al estímulo de las sanas prácticas del crédito- es que, cuando se ha presentado la mora en el cumplimiento de obligaciones de ese tipo, permanezca registrado el dato por un tiempo razonable después de efectuado el pago".

Finalmente el Proyecto de Ley Estatutaria No. 221/2007 de Cámara y No. 027/2006 de Senado, acumulado con el No. 05/2006 Senado, sin definir como lo hicieran otros proyectos de ley lo que debe entenderse por dato negativo y/o dato positivo, procede a enunciar en forma expresa la "información negativa" y en forma tácita la "información positiva", inmersas en los requisitos especiales para las fuentes de información en el artículo 12, y en el extenso régimen de transición previsto en el controvertido artículo 21, respectivamente. Controvertido porque el legislador se preocupó por crear un régimen jurídico y económico inmediateista (una especie de amnistía financiera de tipo legislativo) que para un futuro cierto y relativamente duradero.

Sobre la información negativa se plantea cuando el proyecto de ley hace mención al reporte que deban hacer las fuentes de información a los operadores de información financiera, crediticia, comercial y de servicios, sobre el incumplimiento de obligaciones de cualquier naturaleza. Este reporte sólo procederá: (i) previa comunicación al titular de la información, con el fin de que este pueda demostrar o efectuar el pago de la obligación; y (ii) para controvertir aspectos tales como el monto de la obligación o cuota y la fecha de exigibilidad. Dicha comunicación podrá incluirse en los extractos periódicos que las fuentes de información envíen a sus clientes.

Del amplio régimen de transición previsto en el artículo 21 se infiere los términos de dato negativo y la no menos polémica institución de la "caducidad del dato" ^[108]

El término de caducidad del dato opera en el caso de los titulares de la información, así: (i) que a la entrada en vigencia de este proyecto de ley estuvieren al día en sus obligaciones objeto de reporte, y cuya información negativa hubiere permanecido en los bancos de datos por lo menos un año contado a partir de la cancelación de las obligaciones, serán

(108) En la Sentencia C-687 de 2003, la Corte Constitucional manifestó: "La consagración misma de un término de caducidad implica que el legislador, por medio de un ejercicio de ponderación, resuelve de determinada manera la tensión entre los derechos a la información, al buen nombre y al hábeas data. Igualmente, la consagración de ese término de caducidad es una forma de armonizar el alcance de esos derechos con aspectos medulares de la actividad financiera, que ha sido definida por el constituyente como un bien de interés público de acuerdo al tenor del artículo 335 superior. El legislador, al adoptar esa decisión sobre la caducidad del dato, necesariamente realiza una ponderación entre derechos fundamentales, cuyo resultado deviene inevitablemente, en una regulación de los elementos conceptuales y estructurales mínimos de esos derechos fundamentales, puesto que, como resultado de esa ponderación, es delimitado el contenido constitucionalmente protegido de esos derechos"

beneficiarios de la caducidad inmediata de la información negativa; (ii) que se encuentren al día en sus obligaciones objeto de reporte, pero cuya información negativa no hubiere permanecido en los bancos de datos al menos un año después de canceladas las obligaciones, permanecerán con dicha información negativa por el tiempo que les hiciera falta para cumplir el año, contado a partir de la cancelación de las obligaciones; y (iii) que cancelen sus obligaciones objeto de reporte dentro de los seis (6) meses siguientes a la entrada en vigencia de la presente ley, permanecerán con dicha información negativa en los bancos de datos por el término de un (1) año, contado a partir de la fecha de cancelación de tales obligaciones. Cumplido este plazo de un (1) año, el dato negativo deberá ser retirado automáticamente de los bancos de datos.

La Ley de Habeas Data de 2008, abandona toda definición a datos negativos o positivos, pero incluye en algunos artículos los términos “información negativa” o “información de carácter positivo” que entendemos son sinónimos de datos negativos o datos positivos. De otra parte sobre la caducidad del *dato financiero negativo* previsto en el artículo 21 de la Ley, es declarado exequible por la Corte Constitucional mediante Sentencia C-1011-2008 ^[109].

En efecto, en el Artículo 10, segunda parte del párrafo 1º de la Ley de Habeas Data de 2008, hace mención a “la información negativa”, de la siguiente manera: “La administración de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, por parte de fuentes, usuarios y operadores deberá realizarse de forma que permita favorecer los fines de expansión y democratización del crédito. Los usuarios de este tipo de información deberán valorar este tipo de información en forma concurrente con otros factores o elementos de juicio que técnicamente inciden en el estudio de riesgo y el análisis crediticio, y no podrán basarse exclusivamente en la información relativa al incumplimiento de obligaciones suministrada por los operadores para adoptar decisiones frente a solicitudes de crédito.

*La Superintendencia Financiera de Colombia podrá imponer las sanciones previstas en la presente ley a los usuarios de la información que nieguen una solicitud de crédito basados exclusivamente en el reporte de **información negativa** del solicitante”.*

Por su parte, el artículo 12 de la Ley citada, sobre los requisitos especiales para las “fuentes de información” y especialmente referida a la actualización de información de las fuentes respecto de los operadores de información, establece: “El reporte de **información negativa** sobre incumplimiento de obligaciones de cualquier naturaleza, que hagan las fuentes de información a los operadores de bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, sólo procederá previa comunicación al titular de la información, con el fin de que este pueda demostrar o efectuar el pago de la obligación, así como controvertir aspectos tales como el monto de

(109) La Corte al respecto sostiene: “En conclusión, la caducidad especial del dato financiero negativo prevista en el artículo 21 del Proyecto de Ley es compatible con el ejercicio de las actividades de recolección, tratamiento y circulación de datos personales de contenido crediticio. Igualmente, en tanto tiene un carácter excepcional, limitado en el tiempo y específico, no involucra una afectación desproporcionada del derecho a la información de las entidades que integran el sistema de crédito, ni tampoco tiene un alcance tal que comprometa la estabilidad financiera, amén de la intangibilidad de los demás factores que permiten identificar el nivel de riesgo crediticio y la existencia de un término cierto de permanencia del dato financiero negativo, periodo dentro del cual los agentes económicos pueden acceder a dicha información. En suma, se trata de una medida de intervención económica que busca propósitos constitucionalmente legítimos, respetuosa de los derechos de los sujetos que concurren en la administración de datos personales. Por ende, la norma no se opone a los postulados de la Carta Política y será declarada exequible”

la obligación o cuota y la fecha de exigibilidad. Dicha comunicación podrá incluirse en los extractos periódicos que las fuentes de información envíen a sus clientes”.

Finalmente, el artículo 21 de la citada ley y referido al “régimen de transición” y la “caducidad del dato financiero”, es del mismo tenor y términos allí estipulados para la caducidad de la información negativa, tal como venía desde el proyecto de Ley Estatutaria acumulado de 2006-2007, con la sola diferencia que en la parte in fine del artículo se adicionó lo siguiente: *“El beneficio previsto en este artículo se perderá en caso que el titular de la información incurra nuevamente en mora, evento en el cual su reporte reflejará nuevamente la totalidad de los incumplimientos pasados, en los términos previstos en el artículo 13 de esta ley”,* es decir, *“La **información de carácter positivo** permanecerá de manera indefinida en los bancos de datos de los operadores de información. Los datos cuyo contenido haga referencia al tiempo de mora, tipo de cobro, estado de la cartera, y en general, aquellos datos referentes a una situación de incumplimiento de obligaciones, se regirán por un término máximo de permanencia, vencido el cual deberá ser retirada de los bancos de datos por el operador, de forma que los usuarios no puedan acceder o consultar dicha información. El término de permanencia de esta información será de cuatro (4) años contados a partir de la fecha en que sean pagadas las cuotas vencidas o sea pagada la obligación vencida”.*

3.2.2.2. El Dato o información pública

El Proyecto de Ley Estatutaria No.071 de 2005, en el artículo 5º -12, al referirse al dato público lo definió como aquel dato *“calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados, de conformidad con la presente ley. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas, que no estén sometidos a reserva y los relativos al estado civil de las personas. La administración de información pública no requiere autorización del titular de los datos, pero se sujeta al cumplimiento de los principios de la administración de datos personales y a las demás disposiciones de la misma”.*

Se infiere que existe dato público según el proyecto en los siguientes eventos: (i) Los calificados como tales por el Ordenamiento jurídico vigente; y, (ii) Los datos contenidos en documentos públicos, sentencias judiciales no sometidas a reserva y los documentos contentivos del estado civil de las personas.

Esta técnica remisoría y asimiladora de dato público, a la normatividad vigente y a documentos públicos, respectivamente, no es del todo confiable, máxime que en la Constitución y las leyes no se habla de datos o informaciones personales, ni menos de carácter público y sí a los “documentos públicos” en la Constitución (sólo artículos 74 y al “documento privado” en el artículo 15 in fine) y en algunas leyes como por ejemplo, la Ley 57 de 1985, “Estatuto de la Información Pública”; el Código de Procedimiento Administrativo y Contencioso Administrativo o C.P.A. y C.A; el Código de Procedimiento Penal o C.P.P., el Código de Procedimiento Civil o C.P.C. e incluso los códigos sustantivos Civil, laboral o comercial, entre otros, se refieren a los “documentos públicos” y “documentos privados”.

Pero lo que más llama la atención es la parte final de la definición de dato público, pues en ella se sostiene que quienes administren la información pública, se entiende en un banco o base de datos informatizada o no, obviamente de carácter público, no requerirán de la “autorización del titular de los datos”, es decir, no necesitarán del consentimiento del concernido para la recolección y posterior sometimiento a tratamiento de datos e incluso

para comunicarlos a terceros. Esto atenta contra la autonomía y libre desarrollo de la personalidad (artículo 16 constitucional) y el derecho a la intimidad, buen nombre y el honor previstos en el artículo 15 constitucional. Pues ni siquiera la prevención que toma el proyecto de ley de 2005, al final del artículo citado, minimiza el efecto vulnerador de la Constitución, ya que si los datos son tratados conforme a los demás principios del procesamiento de datos diferente al del consentimiento que es piedra angular en todo Estado con leyes reguladoras del Hábeas Data, resultan inanes los demás principios.

El Proyecto de Ley Estatutaria No. 221/2007 de Cámara y No. 027/2006 de Senado, acumulado con el No. 05/2006 Senado, define en el artículo 3º, literal f), al dato público como aquel *“dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semi-privados o privados, de conformidad con la presente ley. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas”*.

Para la definición de dato público, el proyecto de ley estatutaria recurre a la remisión normativa constitucional y legislativa, en el entendido que toda información de carácter público que se refiera a datos de las personas naturales o jurídicas y sean producto de tratamiento o procesamiento de datos informatizado o no (recolección, selección, almacenamiento, registro, conservación y comunicación), podrían catalogarse como dato público. El legislador difiere esta calificación a la doctrina y a la jurisprudencia colombiana. Para ello, no deberá ab initio, asimilar el término documento público previsto en la Constitución y las leyes (v.gr. Ley 57 de 1985, 692 de 2005, C.C.A., C.P.P. o C.P.C) a dato público, pues como hemos sostenido antes, éste será producto del tratamiento de datos personales previsto en el artículo 15º incisos 1º y 2º constitucional y desarrollado en la norma legislativa respectiva.

Dicho esto, puede presentar serias dudas que las sentencias judiciales y los documentos contentivos de la certificación de estado civil de las personas, *per se* sean datos públicos, sino se demuestra el tratamiento de datos y su incorporación a bancos de datos informatizados o no.

La Directiva Comunitaria 95/46/CE, reconoce que pueden someterse a tratamiento o procesamiento de datos los datos relativos a las infracciones, condenas penales o medidas de seguridad, bajo el control de los poderes públicos y si hay garantías específicas en el derecho nacional. Esto se recoge en la LOPD de España de 1999, artículo 7-6. Obsérvese que no son las sentencias las que son objeto del tratamiento de datos sino los datos incorporados en ellas y más concretamente las que revelen las infracciones, condenas o medidas de seguridad.

Por fortuna el proyecto de ley estatutaria de 2006-2007, eliminó la última parte del artículo que imponía el arrasamiento del principio del consentimiento del concernido para el tratamiento de datos públicos, con la sola excepción de los documentos públicos calificados de reservados por el ordenamiento jurídico vigente.

Finalmente el proyecto de ley estatutaria dentro del cuadro de principios que ofrecen un velo protector a los datos personales en fase de comunicación a terceros o los usuarios, pero en tratándose de los datos públicos, con base en el principio de circulación restringida de datos (el artículo 4º, literal c.), sostiene: *“... no podrán ser accesibles por Internet o por otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los titulares o los usuarios autorizados conforme a la presente ley”*

La Ley 1266 de 2008, en el artículo 3º, literal f), y en el artículo 4º, literal c), recogió en toda su extensión tanto la conceptualización de dato público como velo protector de los datos personales en ciclo de transmisión a terceros o usuarios y sobre la circulación restringida de los datos públicos por vía informática, electrónica o telemática. En efecto, la parte final del literal c, del artículo 4º sostiene: *“Los datos personales, salvo la información pública, no podrán ser accesibles por Internet o por otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los titulares o los usuarios autorizados conforme a la presente ley”*.

3.2.2.3. El Dato semi-privado

El Proyecto de Ley Estatutaria No. 221/2007 de Cámara y No. 027/2006 de Senado, acumulado con el No. 05/2006 Senado, define al dato semi-privado, en el artículo 5º, literal g, como aquel dato *“que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios...”*.

Se define éste clase de datos por deducción lógica de lo que no es y por con el ejemplo aparentemente único del dato financiero que incluye al dato comercial, bancario, bursátil, tributario, fiscal o tarifario, como hemos sostenido anteriormente. Esta clasificación parecería estar mal informando al operador jurídico de la norma que es una especie de dato personal sui generis del cual es “propietario” su titular, pero no solo le interesa a él sino a “cierto sector o grupo de personas o a la sociedad en general”, es decir, a todo el mundo, pero tan solo un poquito a él que paradójicamente es su titular concernido. Lo que no parece bien es que la norma al igual que lo hacía el centenario Código Civil Colombiano, explicaba las normas con ejemplos o casos ejemplarizantes (casuística). Esa técnica legislativa casi cerrada conlleva una pobre aplicabilidad general a diversos sucesos o eventos a los cuales podría estar dirigida.

En el proyecto de ley estatutaria No. 071 de 2005, se denominaba al dato semi-privado en la forma que lo hizo en el anterior proyecto, con la pequeña gran diferencia, que al final de la definición incorporaba aquello que en buena hora se eliminó en el año 2006-2007, es decir, que no se requería de “autorización del titular” para tratar o procesar esta especie de datos personales.

El artículo 3º, literal g), de la Ley 1266 de 2008, retoma la definición de dato semi-privado del proyecto de ley Estatutaria Acumulado de 2006-2007 y lo plasma así: *“Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios a que se refiere el Título IV de la presente ley”*.

El Título IV de la ley citada, se refiere *“a los bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países”*. En este Título se abordan los aspectos medulares del Habeas Data Financiero, tales como el principio de favorecimiento a una actividad de interés público (“democratización del crédito”), los requisitos especiales para las fuentes de información, los requisitos especiales para los operadores de la información, permanencia y contenido de la información, y acceso a la información financiera por parte de los usuarios (artículos 10 a 15 ibídem).

3.2.2.4. Dato privado

El Proyecto de Ley estatutaria No. 071 de 2005, define al dato en el artículo 5º, numeral 14, como aquel “*dato que por su contenido o su naturaleza sólo es relevante para el titular y no puede ser suministrado a terceros o usuarios, sino con su previa autorización. Son datos privados los datos sensibles y los datos íntimos. No podrá divulgarse o suministrarse un dato privado sin el consentimiento previo del titular, salvo las excepciones previstas en la ley*”.

Esta calificación de dato privado encierra dos categorías especiales de datos que en el derecho continental europeo, como se dijo antes, tiene una protección reforzada porque implica nada más ni nada menos que los datos del famoso “núcleo duro” de la *privacy* anglosajona y por tanto, susceptible de máxima protección por parte del Estado. Así lo entendió el proyecto de ley de 2005, al imponer como requisito fundamental para tratar estos datos el consentimiento o autorización previa, expresa y escrita del concernido, sobre todo cuando se somete el dato a la fase de comunicación a terceros o usuarios.

Por su parte, el Proyecto de Ley Estatutaria No. 221/2007 de Cámara y No. 027/2006 de Senado, acumulado con el No. 05/2006 Senado, en forma aparentemente simple define en el artículo 5º literal h, al dato privado como aquel dato “*que por su naturaleza íntima o reservada sólo es relevante para el titular*”. Es aparente, porque aunque elimina la calidad de dato sensible al privado le otorga otra candado de mayor seguridad que éste, cual es denominarlo como dato reservado. Y es la Constitución y las leyes especiales, como la Ley 57 de 1985, la que califica que es o no información reservada. Lo es por ejemplo, las investigaciones penales, las historias clínicas o médicas de una persona, etc.

Solo para ver hasta donde se extiende el concepto de dato privado, digamos lo siguiente:

Un ser humano desde antes de nacer, luego con su nacimiento, crecimiento, desarrollo, muerte, y aún después de ésta, produce una serie de actos, hechos, sucesos susceptibles de documentación (certificados de cualquier tipo y finalidad, registros públicos y privados, obligaciones y contratos, etc); en fin, de informaciones y datos personales, familiares y sociales, los cuales, en mayor o menor grado son sujeto u objeto del derecho y en mayores proporciones de la vida cotidiana, al ser puros y simples y reveladores de la *venida*, paso y extinción de la *vitae humanum*.

El status del *nasciturus* de la persona natural o física y el del *post mortem* en el derecho genera una gran cantidad de información o datos de carácter personal y familiar, tanto escritas, gráficas, auditivas, video auditivas como producidas, captadas, reproducidas, transferidas o consultadas por cualquier medio, dispositivo, aparato mecánico, eléctrico o electromagnético conocido o conocible, muchos de los cuales tienen relevancia en el derecho, dependiendo de diferentes variables que van desde las estrictamente biológicas (v.gr .nacimiento), pasando por las simplemente materiales u objetivas hasta las más sofisticadas que actualmente se conocen, cuando crean, modifican o extinguen situaciones jurídicas individuales o concretas, o generales y abstractas, produciendo derechos, deberes y obligaciones para una persona. Una auscultación médica mediante la técnica de rayos X o cualquiera otra de índole computarizada (p.e. TAC) o de examen de líquidos humanos (orina, sangre, semen, etc) o incluso de partes del cuerpo humano (v.gr. huellas digitales o plantares); cualquier número o símbolo que identifique o se le asigne a una persona (v.gr. documento de identidad personal, profesional, documento de conducción, etc); la información sobre la raza, origen étnico, color, religión, edad o estado civil o sobre la educación, su historial laboral, delictivo, incluso las ideas u opiniones personales sobre otra persona, salvo las vertidas con ocasión de un concurso, premio o subvención según la *Act*

Privacy Canadiense; entre muchas otras relacionadas en un gran listado que no distingue categorías especiales entre aquéllas, constituyen información personal, entendiéndose como tal, la que le concierne a una persona, cualesquiera sean los mecanismos o tecnologías de las que se obtengan o graben.

La Ley de Habeas Data financiero de 2008, en el literal h), del artículo 3º, retoma la conceptualización de dato privado suministrada por el proyecto de Ley Estatutaria Acumulado de 2006-2007. Pero como se dijo antes, la citada ley no precave que en un dato privado, considerado anodino desde su concepción, pues “sólo interesa a su titular”, se traslapa un dato sensible que puede significar para la persona más insidioso a su dignidad humana y a su existencia misma que un dato financiero o semi-privado con valor crematístico que definitivamente parece más proteger esta Ley sectorial de Habeas Data.

3.2.2.5. Información financiera, crediticia, comercial, de servicios y la proveniente de terceros países

Según el literal j, del el Proyecto de Ley Estatutaria No. 221/2007 de Cámara y No. 027/2006 de Senado, acumulado con el No. 05/2006 Senado, se “entenderá por información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, aquella referida al nacimiento, ejecución y extinción de obligaciones dinerarias, independientemente de la naturaleza del contrato que les dé origen, así como la información relativa a las demás actividades propias del sector financiero o sobre el manejo financiero o los estados financieros del titular” (Inexequible según la Sentencia C-1011-2008, artículo 2º in fine).

Como se dijo, la Ley 1266 de 2008, en el literal j), del artículo 3º retoma la anterior definición con un ligero retoque de redacción y la exclusión del aparte declarado inexequible, con lo cual trata de solapar la conceptualización global o generalizada que pudiera tener la denominada “información financiera”, para decir que sólo “a los efectos de la presente ley...” se entenderá su aplicabilidad. En lo demás retoma el texto del proyecto acumulado de 2006-2007.

3.2.2.6. Banco, Base, Registro o Fichero de datos personales

Las leyes europeas como latinoamericanas, respecto de la definición de banco de datos personales son unívocas. En lo que se diferencian las diferentes legislaciones es en el acomodamiento gramatical de lo que entendemos genéricamente, como “conjunto organizado de registros o datos referentes a personas determinadas o determinables, cualquiera que sea la forma, (informatizado o no) los procedimientos o la finalidad del registro” (Proyecto de Ley estatutaria No. 064 de 2003, artículo 5º). En los proyectos de ley estatutaria que incluían esta definición lo denominaban “Banco de Datos”, en igual forma los proyectos de ley estatutaria de 2003 hasta 2007, aunque en estos no incluían una definición técnico-jurídica en el capítulo correspondiente referida al Banco de datos.

En Francia se denomina “*Fichiers*” o fichero de datos; para los anglosajones es el *Bank of date* o “*database*”. En España en la LOPDP indistintamente se denomina Banco, Base o fichero de datos. En la mayor parte de Estados latinoamericanos Banco o Base de datos. Cualquiera sea el nombre, la definición antes suministrada es, altamente comprensible de lo que se quiere significar y entender.

Según el tipo de información o datos que se maneje adoptarán unos apellidos que ejemplifican el objetivo y la finalidad de los mismos: Banco de datos jurídico, Bancos de datos documentarios o documentales ^[110], Bancos de datos financiero, Banco de datos de Salud,

etc. Los bancos de datos jurídicos, a su vez, pueden ser: jurisprudenciales, doctrinales, legislativos o parlamentarios, de las administraciones públicas municipales, distritales, departamentales y nacionales. Según las leyes protectoras de datos personales o del Hábeas Data, se clasifican como bancos de titularidad pública y bancos de titularidad privada (El caso de España, Argentina, Chile, entre otros).

El proyecto de ley estatutaria de 2005 “*Por el cual se dictan disposiciones para la protección de datos de carácter personal y se regula la actividad de recolección, tratamiento y circulación de los mismos*”, preparado a iniciativa de la Defensoría del Pueblo, es quizá el documento doctrinal, porque no se convirtió en ley, que quizá trabajo con más ahínco que cualquiera otro, sobre la clasificación, nominación, objetivos y finalidades. Por eso veamos brevemente lo que allí se manifestaba. Se definía en el artículo 5-5, al *Banco de datos de carácter personal*, como “*el conjunto organizado de registros o datos referentes a personas determinadas o determinables, cualquiera que sea la forma, los procedimientos o la finalidad del registro*”. Luego clasificó a los Bancos de datos como de naturaleza privada (artículos 40 a 52)^[111] y de naturaleza pública (artículos 53 a 62)^[112].

Dentro de los Bancos de Datos de naturaleza privada incluyó a los Bancos de datos de información sobre solvencia patrimonial y financiera (artículos 48 a 52)^[113]; y dentro de los

-
- (110) La incorporación de los bancos de datos en el mundo de la reglamentación jurídica es relativamente reciente. El Banco de Datos es una estructura lógica de acceso, almacenamiento y recuperación de información, y por tanto, no puede ser sólo un simple “*depósito común de documentación, útil para diferentes usuarios y distintas aplicaciones*” (DAVARA, Ángel. Derecho Informático. Pamplona, España, 1997, p. 133), puesto que disponen de un lenguaje propio construido para lograr la identidad literal o conceptual entre el vocabulario utilizado por el usuario de un banco de datos, y del documento que pretende consultar (la estructuración de un Thesaurus). Esto pone de manifiesto la magnitud de la tarea que se pretende emprender para elaborarlo, y su complejidad, pero a la vez pone de relieve su importancia. Podemos afirmar sin lugar a dudas que de la adecuada construcción del Thesaurus depende en gran medida la eficacia de un banco de datos de carácter documental (GIRALDO, Jaime. Informática jurídica documental, Temis, Bogotá, 1990, p. 10). En: ***EL derecho a la intimidad, la visión ius-informática y los delitos relativos a los datos personales***. Tesis Doctoral, Universidad de Lleida (España), Lleida, 1999, p. 405
- (111) Para la creación de bancos de datos de naturaleza privada, las personas jurídicas deberán constituirse como sociedades comerciales, entidades sin ánimo de lucro o entidades cooperativas, con sujeción a los requisitos constitucionales y legales previstos para el efecto. Los operadores deberán contar con adecuados recursos patrimoniales e infraestructura técnica y administrativa suficientes para garantizar la idoneidad del tratamiento y los derechos de los titulares de la información. En el desarrollo de sus actividades, estos bancos de datos deberán obrar de manera que siempre se respeten los derechos y garantías de los titulares de los datos, en especial, su libertad, honra, buen nombre, intimidad personal o familiar y hábeas data, y sin interponer trabas u obstáculos para el ejercicio efectivo de los recursos y acciones que para la protección de sus datos les otorgan la Constitución y la ley. En: www.defensoriapueblo.gov.co
- (112) La creación o modificación de los bancos de datos o centrales de información de las entidades públicas se hará de conformidad con los fines, atribuciones y objeto asignados a la entidad de la cual hacen parte en la norma que haya dispuesto su creación y deberán operar como dependencias del organismo, entidad o establecimiento público del cual hacen parte, con sujeción estricta a los fines, propósitos y facultades previstas en la Constitución, la ley o el acto administrativo que regula su actividad. En: www.defensoriapueblo.gov.co
- (113) Fuentes de información. Las personas jurídicas dedicadas al tratamiento de datos para el suministro de información sobre solvencia patrimonial o sobre cumplimiento e incumplimiento de obligaciones en dinero, sólo podrán obtener datos de fuentes de acceso irrestricto al público o facilitados por el titular directamente al banco de datos o al banco, entidad crediticia, aseguradora, financiera o establecimiento comercial con el cual ha celebrado el contrato respectivo, con su consentimiento previo, expreso, escrito e informado.
Parágrafo. La cesión o divulgación de datos de carácter personal debe hacerse de manera tal que siempre quede registro por cualquier medio idóneo de los reportes que hagan los bancos de datos, los usuarios o las fuentes de información en desarrollo del tratamiento de los datos. En: www.defensoriapueblo.gov.co

bancos de datos de naturaleza pública, incorporó a los bancos de datos de la fuerza pública, policía judicial y organismos de seguridad del Estado (artículos 60 a 62)^[114].

Reguló en forma exclusiva “*las categorías especiales de datos*” (artículos 63 a 67), previa aclaración de que “Ninguna persona puede ser obligada a proporcionar datos sensibles” y que “*los datos sensibles sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por la ley o de interés particular cuando su acopio, uso o divulgación sean necesarios para la protección o promoción de los derechos fundamentales del titular de ellos, siempre que medie su consentimiento expreso y escrito*”; y finalmente que “*podrán ser tratados con finalidades históricas, estadísticas o científicas, adoptando las medidas conducentes a la supresión de identidad de los titulares*”.

Entre esta clase especial de bancos de datos, reguló los siguientes:

1. **Datos sobre la salud.** Los datos relativos a las condiciones de salud, uso de determinados medicamentos, bebidas o sustancias, comportamientos, hábitos o características sexuales, o aquellos consignados en la historia clínica, sólo podrán formar parte de bancos de datos internos de las personas naturales o jurídicas autorizadas para desarrollar actividades de diagnóstico, tratamiento y restablecimiento de la salud, y únicamente podrán ser tratados con exclusivos fines científicos, de administración médica, terapéuticos o de investigación.

2. **Bancos de datos de encuestas o investigaciones.** El tratamiento automatizado de datos de carácter personal para encuestas o investigaciones de carácter estrictamente académico, científico o estadístico legalmente autorizado, requiere el consentimiento libre, expreso e informado de su titular y la observancia de las garantías y derechos consagrados en el ordenamiento vigente. Es obligatorio mantener el anonimato y reserva de identidad de la persona mediante la disociación de sus datos.

3. **Bancos de datos de suscriptores de servicios públicos.** Los bancos de datos de suscriptores de servicios públicos domiciliarios podrán acopiar, registrar y tratar la información de los usuarios para los fines propios de la gestión de la empresa, sin que les sea dable comercializar dicha información, salvo las excepciones previstas en esta ley. En los respectivos directorios de circulación pública podrán aparecer los nombres y números de los suscriptores de servicios públicos domiciliarios, salvo que el titular exija su exclusión.

4. **Bancos de datos con fines de publicidad y ventas.** Para el desarrollo de actividades con fines comerciales, promocionales o publicitarios, se podrán tratar datos que sean aptos para establecer hábitos de consumo, cuando éstos figuren en documentos accesibles al público o hayan sido facilitados por los propios titulares u obtenidos con su consentimiento.

El titular podrá en cualquier momento solicitar el retiro de su nombre de los bancos de datos a los que se refiere el presente artículo.

(114) Sujeción al régimen general. Los bancos de datos a cargo de los cuerpos, entidades u organismos que integran la fuerza pública, de policía judicial o de seguridad del Estado se regirán en lo pertinente por las normas y principios consagrados en esta ley, sin perjuicio de las normas especiales que regulan las actividades propias de sus respectivas competencias institucionales y dejando a salvo la reserva legal prevista para ciertas actuaciones. El Gobierno Nacional podrá expedir las reglamentaciones que, con sujeción estricta a las normas, principios y derechos que consagra esta ley, se requieran para el adecuado desarrollo de las actividades de estos bancos de datos. En: www.defensoriapueblo.gov.co

En los documentos de publicidad, ventas y actividades análogas, la firma que promociona o comercializa un bien, servicio o producto, deberá indicar en el documento respectivo la fuente de la cual ha obtenido los datos del destinatario.

La Ley 1266 de 2008, se apartó de las conceptualizaciones de “Banco”, “fichero” o “Base” de datos, así como de su amplia clasificación y regímenes jurídicos aplicables y excepciones al mismo, que el único proyecto integral de habeas data en Colombia de 2005, presentado por la Defensoría del Pueblo había estipulado en su larga lista de conceptualizaciones preliminares del proyecto para poder entender en contenido ius tecnológico de la institución jurídico del Habeas Data, así como en su régimen jurídico y excepciones de aplicabilidad del mentado proyecto de ley.

Sin embargo, a lo largo de la mentada ley encontramos la utilización de los términos: “banco de datos” para referirse a un conjunto de datos o informaciones que han sido procesados o tratados mediante medios informáticos por personas autorizadas y tienen relevancia jurídica y sobre todo “financiera” y de los cuales se infieren derechos y deberes para los titulares o personas concernidas como para quienes los operan, administran o quienes los suministraron.

En efecto, los términos “Bancos de datos” los encontramos desde el inicio hasta la terminación del texto legal. Se inicia diciendo en el artículo 2º de la ley, sobre el ámbito de aplicación de la ley que ésta “*se aplica a todos los datos de información personal registrados en un **banco de datos**, sean estos administrados por entidades de naturaleza pública o privada*”.

Se termina aludiendo a los bancos de datos, al referirse el artículo 18 de la mentada ley, a las sanciones que imponen la Superintendencia de Industria y Comercio y la Superintendencia Financiera, según fuere el caso, a los operadores, fuentes o usuarios de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países previas explicaciones de acuerdo con el procedimiento aplicable, las siguientes sanciones: (i) Multas de carácter personal o institucional; (ii) *Suspensión de las actividades del banco de datos*, hasta por un término de seis (6) meses, cuando se estuviere llevando a cabo la administración de la información en violación grave de las condiciones y requisitos previstos en la presente ley, así como por la inobservancia de las órdenes e instrucciones impartidas por las Superintendencias mencionadas para corregir tales violaciones; y, (iii) *Cierre o clausura de operaciones del banco de datos* cuando, una vez transcurrido el término de suspensión, no hubiere adecuado su operación técnica y logística, y sus normas y procedimientos a los requisitos de ley, de conformidad con lo dispuesto en la resolución que ordenó la suspensión. Cierre inmediato y definitivo de la operación de bancos de datos que administren datos prohibidos.

3.3. Elementos formales

Para que una persona concernida con los datos personales que se hayan recabado en una base o banco de datos pueda solicitar a los responsables de la administración, coordinación dirección de los mismos, sean éstos públicos o privados, la actualización, rectificación o eliminación de los datos inexactos, erróneos, incompletos, “antiguos”, “discriminatorios”, falsos o no conformes al ordenamiento jurídico vigente, el “interesado, afectado” o titular de los datos dispone según la legislación europea o latinoamericana aplicable al caso, de mecanismos administrativos (derecho de petición, recursos administrativos ordinarios o extraordinarios o recurso o acciones de Hábeas data administrativo) o jurisdiccionales (recurso, acción, garantía o “proceso” constitucional y legal de Hábeas Data), para que el Estado o las personas, entidades u organismos de

carácter privado tutele sus derechos de la intimidad, el honor, la honra, el buen nombre, la imagen, la voz, la reputación e incluso el mismo derecho a la información desde la arista de la facultad que tiene toda persona para controlar el uso, conservación y finalidad que se da a sus propios datos como la de recibir información oportuna y veraz.

La Corte constitucional colombiana ha sostenido que el núcleo esencial del derecho al Hábeas Data, *“está integrado por el derecho a la autodeterminación informática y por la libertad en general y en especial la económica. La autodeterminación le confiere una facultad o un derecho a la persona a la cual se refieren los datos, para autorizar su conservación, uso y circulación, de acuerdo con las regulaciones legales sobre la materia...”* ^[115].

“El derecho a la autodeterminación informática constituye la facultad de una persona para autorizar la recolección, conservación, uso y circulación de los datos existentes en una base de datos pública o privada, así como para conocerla, actualizarla, rectificarla o cancelarla, y también determinar por sí misma, cuándo y dentro de qué límites, pueden revelarse situaciones referentes a su propia vida” ^[116].

Respecto de la libertad como parte del núcleo esencial, la Corte Constitucional ha recordado que ésta nace bajo la *“égida del derecho general de libertad (artículo 16) y la cláusula específica de libertad en el manejo de los datos (artículo 15 primer inciso)”* ^[117], es decir, afincada en el derecho a la autonomía personal o el libre desarrollo de la personalidad, en general o el derecho a la libertad del concernido con los datos personales a controlar la recolección, tratamiento y circulación de los datos.

El actual derecho fundamental y garantía constitucional de Hábeas Data que en la primera etapa jurisprudencial de estructuración (1992 a 1997), se considerada *“un derecho innominado a conocer, actualizar y rectificar informaciones recogidas en archivos y bancos de datos”* ^[118] previsto en el artículo 15º incisos 1º y 2º de la Constitución colombiana, y que al escindirse del derecho de la intimidad y el buen nombre, se consagró como un derecho autónomo que la Corte Constitucional no dudó jamás en denominarlo derecho de Hábeas Data o derecho de autodeterminación informática, con las mismas facultades ^[119], atributos o derechos componentes: el conocimiento y acceso a la información, actualización, rectificación y eliminación de datos del concernido o del titular de los datos.

La Ley 1266 de 2008, en el artículo 1º al exponer el objeto de la ley hace alusión a la esencia del derecho de habeas data, así como sus facultades para quienes son titulares de datos personales que eventual o definitivamente puedan ser vulnerados. Se inicia enfatizando en el concepto de habeas data sin explicitarlo cuando sostiene: *“el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos, y los demás derechos, libertades y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales a que se refiere el artículo 15 de la Constitución Política, así como el derecho a la información establecido en el artículo 20 de la Constitución Política, particularmente en relación con la información financiera y*

(115) Sentencias T-527-2000, T-578-2001, T-257-2002, T-268-2002.

(116) DURAN RIBERA, Willman R. **Contenido y alcances del Hábeas Data en Bolivia**. En: <http://www.tribunalconstitucional.gov.bo/>

(117) Corte Constitucional, T-729-2002, Septiembre 5

(118) Corte Constitucional, T-414-92 citada en la sentencia T-729-2002, Septiembre 5

(119) Corte Constitucional, SU-082-1995.

crediticia, comercial, de servicios y la proveniente de terceros países". Al final como no era menos se culmina con el epicentro de la Ley sectorial de Habeas Data: el dato financiero.

3.3.1. Conocimiento de la Información

3.3.1.1. En la normatividad comunitaria y española

La legislación comunitaria europea, más concretamente la Directiva 95/46/CE, reconoce el derecho a la información que le asiste al "interesado", concierne o titular de los datos en dos situaciones: (i) Cuando la Información ha sido obtenida de datos recabados del propio interesado; y (ii) Cuando la información no ha sido recabada del propio interesado.

En el primer caso, los Estados miembros dispondrán que el responsable del tratamiento o sus representantes, deberán comunicar a la persona de quien se recaben los datos que le concierne, cuando menos la siguiente información, salvo que ya estuviese informado de ella: (i) La identidad del responsable del tratamiento y, en su caso, de su representante; (ii) Los fines del tratamiento de que van a ser objeto los datos; (iii) Cualquiera otra información tal como: a. Los destinatarios o las categorías de destinatarios de los datos; b. el carácter obligatorio o no de la respuesta y las consecuencias que tendría para la persona interesada una negativa a responder; c. La existencia de derechos de acceso y rectificación de los datos que la conciernen.

En el segundo caso, los Estados miembros dispondrán que el responsable del tratamiento o su representante deberán, desde el momento del registro de los datos o, en caso de que se piense comunicar datos a un tercero, a más tardar, en el momento de la primera comunicación de datos, comunicar al interesado por lo menos la información relatada en el primer caso (*i a iii*), salvo que el interesado ya hubiese sido informado sobre aquello.

Aclara la Directiva comunitaria en éste segundo caso, que estas facultades que tiene el concierne con la información, no se aplicarán, en particular en los siguientes casos: (i) para el tratamiento con fines estadísticos o de investigación histórica o científica; (ii) cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados; (iii) cuando el registro o la comunicación a un tercero estén expresamente proscritos por la ley. En estos casos los Estados establecerán garantías apropiadas.

El artículo 5 de la LOPD española de 1999, al recoger los directrices de la Norma comunitaria, hace efectivo el derecho de conocimiento de la información aplicada al tratamiento informatizado o no de datos y así lo llama "derecho de la información en la recogida de datos". El derecho se desglosa así:

1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco: (i) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información; (ii) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas; (iii) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos; (iv) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición; (v) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

2. Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior.
3. No será necesaria la información a que se refieren las letras b), c) y d) del apartado 1 si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban.
4. Cuando los datos de carácter personal no hayan sido recabados del interesado, éste deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad, del contenido del tratamiento, de la procedencia de los datos, así como de lo previsto en las letras a), d) y e) del apartado 1 del presente artículo.
5. No será de aplicación lo dispuesto en el apartado anterior: (i) cuando expresamente una Ley lo prevea, cuando el tratamiento tenga fines históricos, estadísticos o científicos; (ii) cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados, a criterio de la Agencia de Protección de Datos o del organismo autonómico equivalente, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias; y (iii) cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, en cuyo caso, en cada comunicación que se dirija al interesado se le informará del origen de los datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten.

3.3.1.2. En la normatividad latinoamericana

La legislación de Americana Latina regula el derecho a la información sobre el tratamiento informatizado o no de datos de forma no tan detallada como en derecho continental europeo. La LPDA de Argentina, por ejemplo regula como derecho de los titulares de los datos el “derecho de información”, el cual está previsto en el artículo 13 y lo tiene “toda persona” para que *“pueda solicitar información al organismo de control relativa a la existencia de los archivos, registros, bases o bancos de datos personales, sus finalidades y la identidad de sus responsables”*.

La Ley No. 19628 de Chile sobre protección a la vida privada o la protección a los datos personales, en el artículo 4º, determina que “el tratamiento de los datos personales sólo puede efectuarse cuando esta ley u otras disposiciones legales lo autoricen o el titular consienta expresamente en ello”. Y agrega: “La persona que autoriza debe ser debidamente informada respecto del propósito del almacenamiento de sus datos personales y su posible comunicación al públicoLa autorización debe constar por escrito.”.

No requiere de esta autorización en los siguientes casos: (i) cuando el tratamiento de datos personales que provengan o que se recolecten de fuentes accesibles al público; (ii) cuando sean de carácter económico, financiero, bancario o comercial; (iii) se contengan en listados relativos a una categoría de personas que se limiten a indicar antecedentes tales como la pertenencia del individuo a ese grupo, su profesión o actividad, sus títulos educativos, dirección o fecha de nacimiento; (iv) sean necesarios para comunicaciones comerciales de respuesta directa, comercialización, venta directa de bienes o servicios; (v) cuando el tratamiento de datos personales lo realicen personas jurídicas privadas

para su uso exclusivo o de los asociados, de las entidades a que están afiliadas, o con fines estadísticos, de tarificación u otros de beneficio general.

En el derecho colombiano constitucionalmente se ha consagrado el derecho a la información en el artículo 20, constitucional tanto en su vertiente activa como pasiva. Con base en esta última y siendo un derecho fundamental de aplicación inmediata que no requiere reglamentación legislativa o administrativa para hacerlo efectivo por quien considere que debe ser informado en forma veraz, oportuna e imparcial del sometimiento a tratamiento informatizado o no de los datos personales que le conciernan, ya sea de los datos suministrados por él mismo o no, o bien se trate por personas o entidades públicas o privadas.

En el Proyecto de Ley Estatutaria No. 221/2007 de Cámara y No. 027/2006 de Senado, acumulado con el No. 05/2006 Senado, el derecho de información del concernido con los datos y el consecuente conocimiento de la misma, en el proyecto de ley estatutaria esta blindado por activa como por pasiva, pues se establece como un derecho para el concernido (titular de la información, artículo 3-a) en los principios que orientan la administración de los datos, particularmente en el principio de veracidad o calidad de los datos (información veraz, completa, exacta, actualizada, comprobable y comprensible), el de finalidad (La finalidad debe informársele al titular de la información previa o concomitantemente con el otorgamiento de la autorización, cuando ella sea necesaria o en general siempre que el titular solicite información al respecto) y el de interpretación integral de los derechos constitucionales (intimidad, buen nombre, imagen, honor e información); así como en los derechos de los titulares de los datos, frente a los operadores de los bancos de datos (artículo 6-1), a las fuentes de información (artículo 6-2) y a los usuarios (artículo 63-). Por pasiva como deberes de los operadores de los bancos de datos, a las fuentes-operadores de información y a los usuarios frente al tratamiento o procesamiento de datos.

Precisamente es deber de los operadores de los bancos de datos o los fuente-operadores de la información, según lo dispone el artículo 7-1, *“Garantizar, en todo tiempo al titular de la información, el pleno y efectivo ejercicio del derecho de hábeas data y de petición, es decir, la posibilidad de conocer la información que sobre él exista o repose en el banco de datos, y solicitar la actualización o corrección de datos, todo lo cual se realizará por conducto de los mecanismos de consultas o reclamos, conforme lo previsto en la presente ley”*.

Según el artículo 9-2, es deber de los usuarios de la información, entre otros: *“Informar a los titulares, a su solicitud, sobre la utilización que le está dando a la información”*.

La Ley 1266 de 2008, recogió en su integridad lo dispuesto por el proyecto acumulado de Ley Estatutaria de 2006-2007, sobre los aspectos comentados de conocimiento de la información (derecho y deber) por el concernido y en ese mismo orden de artículos y numerales.

3.3.2. Para acceder a la información

3.3.2.1. En el ámbito europeo y español

En el derecho comunitario europeo, la Directiva No. 95/46/CE, establece el derecho de acceso el cual debe estar garantizado por los Estados miembros a todos los interesados el derecho a obtener del responsable del tratamiento, lo siguiente: 1. Libremente, sin restricciones y con una periodicidad razonable y sin retrasos ni gastos

excesivos: (i) la confirmación de la existencia o inexistencia del tratamiento de datos que le conciernen, así como la información por lo menos de los fines de dichos tratamientos, las categorías de datos a que se refieran y los destinatarios o las categorías de destinatarios a quienes se comuniquen dichos datos; (ii) La comunicación, en forma inteligible, de los datos objeto de los tratamientos, así como toda la información disponible sobre el origen de los datos; (iii) el conocimiento de la lógica utilizada en los tratamientos automatizados de los datos referidos al interesado al menos en los casos de las decisiones individuales automatizadas (laborales, sobre crédito, fiabilidad, conducta, etc.); 2. En su caso, la rectificación, la supresión o el bloqueo de datos cuyo tratamiento no se ajusta a las disposiciones de la Directiva, en particular a causa del carácter incompleto o inexacto de los datos; 3. La notificación a los terceros a quienes se hayan comunicado los datos de toda rectificación, supresión o bloqueo.

Se establece como excepciones al derecho anterior, para salvaguardar: (i) la seguridad del Estado; (ii) La defensa; (iii) La seguridad Pública; (iv) La prevención, la investigación, la detección y la represión de infracciones penales o de las infracciones de la deontología en las profesiones reglamentadas; (v) Un interés económico y financiero importante de un Estado miembro... incluidos los asuntos monetarios, presupuestales y fiscales; (vi) una función de control, de inspección o reglamentaria relacionada, aunque sólo sea ocasionalmente; (vi) La protección del interesado o de los derechos y libertades de otras personas.

La LOPDP española de 1999, en el artículo 15 reconoce el derecho de acceso, así:

1. El interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos así como las comunicaciones realizadas o que se prevén hacer de los mismos.
2. La información podrá obtenerse mediante la mera consulta de los datos por medio de su visualización, o la indicación de los datos que son objeto de tratamiento mediante escrito, copia, telecopia o fotocopia, certificada o no, en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos.
3. El derecho de acceso a que se refiere este artículo sólo podrá ser ejercitado a intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo al efecto, en cuyo caso podrá ejercitarlo antes.

3.3.2.2. En el ámbito Latinoamericano

En la LPDA de 2000, regula en el artículo 14 el derecho de acceso, por el cual: 1. El titular de los datos, previa acreditación de su identidad, tiene derecho a solicitar y obtener información de sus datos personales incluidos en los bancos de datos públicos, o privados destinados a proveer informes. 2. El responsable o usuario debe proporcionar la información solicitada dentro de los diez días corridos de haber sido intimado fehacientemente. Vencido el plazo sin que se satisfaga el pedido, o si evacuado el informe, éste se estimara insuficiente, quedará expedita la acción de protección de los datos o de Hábeas data. 3. El ejercicio de acceso ejercido el titular es gratuito y a intervalos no inferiores a seis meses, salvo que se acredite un interés legítimo al efecto. 4. El ejercicio de éste derecho en el caso de personas fallecidas le corresponde a sus sucesores universales.

En el derecho colombiano, el derecho de acceso a la información constitucionalmente está previsto en el artículo 20 para la información de carácter privado y el artículo 74 para la información pública. El acceso a la información pública general esta reglamentado en la

Ley 57 de 1985, mediante el cual *“Toda persona tiene derecho a consultar los documentos que reposen en las oficinas públicas y a que se le expida copia de los mismos, siempre que dichos documentos no tengan carácter reservado conforme a la Constitución o la Ley, o no hagan relación a la defensa o seguridad nacional”*.

En el Proyecto de Ley Estatutaria No. 221/2007 de Cámara y No. 027/2006 de Senado, acumulado con el No. 05/2006 Senado. Al igual que el derecho a la información que tiene el titular de los datos frente a los operadores de los bancos de datos, las fuentes de información y los usuarios, el derecho de acceso a la información también se halla regulado como derecho para el titular de los datos y otras personas legalmente habilitadas y también como deber para los responsables de los bancos de datos y los fuentes-operadores de información

Es deber de los operadores de los bancos de datos o fuente-operadores de la información, según el artículo 7-3, *“permitir el acceso a la información únicamente a las personas que, de conformidad con lo previsto en esta ley, pueden tener acceso a ella”*.

La Ley de Habeas Data financiero de 2008, retomó íntegramente este aspecto y en idénticas condiciones y articulado al proyecto de ley comentado.

Según el principio de circulación restringida de la información prevista en el artículo 4º , literal c), el acceso a la información tiene sus matizaciones: *“La administración de datos personales se sujeta a los límites que se derivan de la naturaleza de los datos, de las disposiciones de la presente ley y de los principios de la administración de datos personales especialmente de los principios de temporalidad de la información y la finalidad del banco de datos.*

Los datos personales, salvo la información pública, no podrán ser accesibles por Internet o por otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los titulares o los usuarios autorizados conforme a la presente ley”. Esta excepción como se anotó *ut supra* pretende salvaguardar a los datos personales contra toda intromisión a la intimidad, buen nombre, el honor y demás derechos fundamentales y de carácter legal que pudieran verse comprometidos en la divulgación o comunicación masiva de datos personales, quedan excluidos los datos que hayan sido objeto o tratamiento de disociación o que no puedan identificarse plenamente a una persona.

El artículo 15 de la mentada ley garantiza el acceso a la información por parte de los usuarios en los siguientes términos: *“La información contenida en bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países podrá ser accedida por los usuarios únicamente con las siguientes finalidades: Como elemento de análisis para establecer y mantener una relación contractual, cualquiera que sea su naturaleza, así como para la evaluación de los riesgos derivados de una relación contractual vigente.*

Como elemento de análisis para hacer estudios de mercado o investigaciones comerciales o estadísticas.

Para el adelantamiento de cualquier trámite ante una autoridad pública o una persona privada, respecto del cual dicha información resulte pertinente”.

Para cualquier otra finalidad, diferente de las anteriores, respecto de la cual y en forma general o para cada caso particular se haya obtenido autorización por parte del titular de la información”.

Sin embargo y por pasiva también se prohíbe el acceso a cierta información negativa, cuando en el artículo 13 al mencionar a la información positiva de los titulares de la misma, hace la aclaración siguiente: *“Los datos cuyo contenido haga referencia al tiempo de mora, tipo de cobro, estado de la cartera, y en general, aquellos datos referentes a una situación de incumplimiento de obligaciones, se registrarán por un término máximo de permanencia, vencido el cual deberá ser retirada de los bancos de datos por el operador, de forma que los usuarios no puedan acceder o consultar dicha información. El término de permanencia de esta información será de cuatro (4) años contados a partir de la fecha en que sean pagadas las cuotas vencidas o sea pagada la obligación vencida”.*

3.3.3. Para actualizar, rectificar o eliminar la información

3.3.3.1. En el ámbito europeo y español

En la LOPDP, en los artículos 16 y 17 se regulan los derechos de rectificación y cancelación de los datos y el procedimiento de oposición (previsto como un derecho del interesado en el artículo 15 de la Directiva Comunitaria), acceso, rectificación y cancelación de los datos.

Respecto del primer aspecto, la LOPDP, sostiene: 1. El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días; 2. Serán rectificadas o canceladas, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la Ley y, en particular, cuando tales datos resulten inexactos o incompletos; 3. La cancelación dará lugar al bloqueo ^[120] de los datos, conservándose únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión; 4. Si los datos rectificadas o cancelados hubieran sido comunicados previamente, el responsable del tratamiento deberá notificar la rectificación o cancelación efectuada a quien se hayan comunicado, en el caso de que se mantenga el tratamiento por este último, que deberá también proceder a la cancelación; 5. Los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado.

En relación con el procedimiento para ejercitar el derecho de oposición, acceso, así como la rectificación y cancelación se rige por las normas reglamentarias dictadas al efecto (Decreto 1558/2001).

(120) “El derecho de cancelación permite eliminar del archivo de datos a aquellos datos personales que, por diversas circunstancias, no deben figurar en el mismo. Es importante poner de manifiesto que el término “cancelación” debe ser entendido en forma amplia como la acción tendiente a hacer irreconocibles los datos archivados, ya sea anulando, destruyendo, borrando, tornando ilegibles o declarando su nulidad. La metodología empleada definirá de acuerdo a las circunstancias. Demás está decir que existen casos en los que, por cuestiones de interés público, será imposible eliminar completamente una información. Prueba de ello es la excepción a la destrucción física de los datos que la ley contempla en diversos artículos al referirse al mecanismo de bloqueo de datos”. Cfr. TANUS, Gustavo Daniel. **Protección de datos personales, principios generales, derechos, deberes y obligaciones**. En: <http://www.protecciondedatos.com.ar>

La ley 1266 de 2008, establece en el artículo 1º, relativo al objetivo de la Ley, que el derecho constitucional de habeas data tiene como característica y fines primordiales el que toda persona pueda: “*conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos...*”. En consecuencia, le asiste a toda persona los derechos no sólo de conocer la información que le concierne y esté almacenada en una base de datos, sino que si ésta es desactualizada, errónea, ilegal, falsa o no se ajusta a la realidad, pueda solicitar su actualización, rectificación y en su caso, la eliminación de la información, bien sea en vía administrativa (habeas data administrativo), o bien sea en vía jurisdiccional (habeas data jurisdiccional).

3.3.3.1. En el ámbito Latinoamericano

En la LPDA argentina de 2000, en el artículo 16 y 17 se regula el derecho a la rectificación, actualización o supresión de los datos personales y las excepciones correspondientes, así:

Es derecho de toda persona solicitar 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. En tales circunstancias, el responsable o usuario del banco de datos, debe proceder a la rectificación, supresión o actualización de los datos personales del afectado, realizando las operaciones necesarias a tal fin en el plazo máximo de cinco días hábiles de recibido el reclamo del titular de los datos o advertido el error o falsedad.

El incumplimiento de esta obligación dentro del término acordado (de 5 días), habilitará al interesado a promover sin más la acción de protección de los datos personales o de hábeas data prevista en la presente ley.

En el supuesto de cesión, o transferencia de datos, el responsable o usuario del banco de datos debe notificar la rectificación o supresión al cesionario dentro del quinto día hábil de efectuado el tratamiento del dato.

La supresión no procede cuando pudiese causar perjuicios a derechos o intereses legítimos de terceros, o cuando existiera una obligación legal de conservar los datos.

Durante el proceso de verificación y rectificación del error o falsedad de la información que se trate, el responsable o usuario del banco de datos deberá o bien bloquear el archivo, o consignar al proveer información relativa al mismo la circunstancia de que se encuentra sometida a revisión.

Los datos personales deben ser conservados durante los plazos previstos en las disposiciones aplicables o en su caso, en las contractuales entre el responsable o usuario del banco de datos y el titular de los datos.

Las excepciones al ejercicio de los derechos del titular de los datos o de las personas habilitadas por la ley para hacerlo, son las siguientes:

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; y 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

En el Proyecto de Ley Estatutaria No. 221/2007 de Cámara y No. 027/2006 de Senado, acumulado con el No. 05/2006 Senado. Al igual que sucede con los derechos de información y de acceso a la misma por parte del titular de los datos frente a los operadores de los bancos de datos, a las fuentes de información y los usuarios, el derecho de actualización, rectificación y eliminación de los datos también se halla regulado como derecho para el titular de los datos y otras personas legalmente habilitadas y también como deber para los responsables de los bancos de datos, las fuentes de información y los fuentes-operadores de información.

Los derechos de actualización, rectificación y eliminación de los datos, a solicitud del titular de los datos, están previstos como deberes de los operadores de los bancos de datos y de los fuente-operadores de la información, así: (i) Realizar periódica y oportunamente la actualización y rectificación de los datos, cada vez que le reporten novedades las fuentes (artículo 7-7); (ii) Tramitar las peticiones, consultas y los reclamos formulados por los titulares de la información, en los términos señalados en la presente ley (artículo 7-8); y (iii) Indicar en el respectivo registro individual que determinada información se encuentra en discusión por parte de su titular, cuando se haya presentado la solicitud de rectificación o actualización de la misma y no haya finalizado dicho trámite, en la forma en que se regula en la presente ley (artículo 7-9).

Por su parte, las fuentes de información en relación con los derechos de actualización, rectificación y eliminación de datos podrán: (i) *ex officio* rectificar la información cuando sea incorrecta e informar lo pertinente a los operadores (artículo 8-3); (ii) Resolver los reclamos y peticiones del titular en la forma en que se regula en la presente ley (artículo 8-7); (iii) Informar al operador que determinada información se encuentra en discusión por parte de su titular, cuando se haya presentado la solicitud de rectificación o actualización de la misma, con el fin de que el operador incluya en el banco de datos una mención en ese sentido hasta que se haya finalizado dicho trámite (artículo 8-8).

La Ley 1266 de 2008, retoma en su integridad anteriores los planteamientos realizados por el proyecto de Ley Estatutaria acumulado de 2006-1007, y recoge así los derechos de los titulares de los datos y los deberes de operadores y fuentes de información sobre la actualización, rectificación y eliminación de los datos personales erróneos, falsos, ilegales y desactualizados.

Por su parte el artículo 11-4 de la Ley citada, al referirse a los requisitos especiales de los operadores de la información de carácter financiero, establece que éstos *“deberán actualizar la información reportada por las fuentes con una periodicidad no superior a diez (10) días calendario contados a partir del recibo de la misma”*, para garantizar el derecho de habeas data en la facultad de actualización de la información si esta es errada, ilegal o desactualizada. Además, *“deberán contar con un sistema de seguridad y con las demás condiciones técnicas suficientes para garantizar la seguridad y actualización de los registros, evitando su adulteración, pérdida, consulta o uso no autorizado conforme lo previsto en la presente ley”* (artículo 11-3 *Ibidem*).

Igualmente, el artículo 12 de la mentada ley como deberes especiales, aparte de los establecidos en el artículo 8º, que “*Las fuentes deberán actualizar mensualmente la información suministrada al operador*”, en aras a garantizar los derechos de los titulares de la información y de los usuarios de la misma.

3.3.4. La Comunicación, “circulación”, “movimiento” o “transferencia” de la información

3.3.4.1. En el derecho comunitario europeo y en el español

La Directiva Comunitaria 95/46/CE, denomina al fenómeno de comunicación o circulación de datos entre países, ya sea apoyados por las tecnologías TIC y la informática o por otros medios convencionales, la “*transferencia de datos personales a países terceros*” (artículos 25 y 26). La LOPDP española de 1999 denomina “*Movimiento internacional de datos*” y “flujo transfronterizo de datos”, según el Convenio de Europa de 1980.

El profesor *Poulet* ^[121], define a los “flujos transfronterizos de datos” sólo dentro de la concepción del Convenio de Europa de 1980, como “*la trasmisión personal o de las informaciones a través de las fronteras políticas y culturales, por el procedimiento de aprovisionamiento en las filas de computadores*”. Por su parte, *Van der Mensbrugghe* ^[122], exalta la conceptualización de Poulet, cuando señala que la transferencia o intercambio de datos “*es vital entre las oficinas de la información, no únicamente por el aporte en el crecimiento internacional de la producción, sino por cuanto facilita la competitividad y la no discriminación. Además es necesario reconocer la interdependencia entre oficinas que tienen incorporada en sus estructuras la informatización de los datos. La importancia de la internacionalización de datos se refuerza por el aumento de los ficheros informatizados y la progresión rápida y sorprendente de las tecnologías*”.

El Convenio Europeo, con base en los considerandos preliminares mencionados reguló en forma específica, en su articulado, todo lo atinente a los “*Flujos transfronterizos de datos*”, pero especialmente, el intercambio electrónico de los datos de carácter personal proporcionando una serie de directrices normativas sobre la materia para los diferentes Estados Europeos suscriptores del Convenio. Sin embargo, dichas guías se plantearon, en parte (nos referimos a lo técnico-jurídica que regulan a los mecanismos “de intercambio electrónico de datos” --EDI-, como anteriormente se ha visto), dentro de una lógica tradicional cuando se hace mención a los “flujos transfronterizos”, recordando los límites geográficos que en la “cultura electrónica” desaparecen. Olvidan los redactores del Convenio que los fenómenos electromagnéticos TIC, se caracterizan principalmente, como lo sostiene el profesor *Ethain* ^[123], por realizarse dentro de marcos, formatos, velocidades electrónicas y sin contextualización de los espacios geográficos. Si el flujo de datos se hace por soportes y medios que no sean los electrónicos, la lógica empleada por el Convenio en este punto es explicable.

La Directiva 95/46/CE., al abordar el tema del flujo electromagnético de datos personales hace referencia a la “*Transferencia de datos personales a países terceros*” (artículo 25),

(121) Citado por Patricia VAN DER MENSBRUGGHE. En: **Flujos transfronterizos de datos en la Directiva 95/46 de las Comunidades Europeas**. En: Revista Actualidad informática Aranzadi. Ed. Aranzadi S.A., No. 20 Julio, Elcano (Navarra), Madrid, 1996, pág. 12

(122) VAN DER MENSBRUGGHE, Patricia. En: **Flujos transfronterizos...** Ob. cit. pág. 13

(123) KATSH, Ethain. **Rights, Camera, Action: Cyberspatial settings and the first amendment**. Professor of Legal Studies, University of Massachusetts at Amherst; B.A. 1967, New York University; J.D. 1970, Yale University. En: www.umontreal.edu.ca.

explicando previamente en los considerandos de la Directiva que los flujos transfronterizos de datos personales son necesarios para el desarrollo del comercio internacional; que la protección de las personas garantizada en la Comunidad por la presente Directiva no se opone a la transferencia de datos personales a terceros países que garanticen un nivel de protección adecuado; que el carácter adecuado del nivel de protección ofrecido por un país tercero debe apreciarse teniendo en cuenta todas las circunstancias relacionadas con la transferencia o la categoría de transferencias (C. 56). Es decir, que se exalta la necesidad imperiosa por parte de los Estados Miembros de la UE., de contemplar la figura del flujo electromagnético de datos personales, con clara observancia de las garantías y niveles y grados de protección de los derechos, libertades públicas e intereses legítimos y las correspondientes acciones para implementar y potenciarlas por los Estados.

Así mismo, se considera necesario garantizar un *mínimum* de excepciones a la regla general del flujo electromagnético de datos en ciertos casos previa y taxativamente enunciados, tales como cuando se esté ante el tratamiento de datos personales con fines periodísticos o de expresión artística o literaria, en particular en el sector audiovisual, siempre que resulten necesarias para conciliar los derechos fundamentales de la persona con la libertad de expresión y, en particular, *la libertad de recibir o comunicar informaciones*, tal y como se garantiza en el artículo 10 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales; que por lo tanto, para ponderar estos derechos fundamentales, corresponde a los Estados miembros prever las excepciones y las restricciones necesarias en lo relativo a las medidas generales sobre la legalidad del tratamiento de datos, *las medidas sobre la transferencia de datos a terceros países* y las competencias de las autoridades de control sin que esto deba inducir, sin embargo, a los Estados miembros a prever excepciones a las medidas que garanticen la seguridad del tratamiento; que, igualmente, debería concederse a la autoridad de control responsable en la materia al menos una serie de competencias *a posteriori* como por ejemplo publicar periódicamente un informe al respecto o bien iniciar procedimientos legales ante las autoridades judiciales.

Bien es cierto, que la Directiva actualiza jurídica como tecnológicamente el concepto de flujo electromagnético de datos personales, pero no cabe duda también, que éste cuerpo normativo comunitario recoge los elementos de conceptualización, estructuración y aplicabilidad suministrados desde la incorporación a la legislación europea del Convenio de Estrasburgo de 1981, sobre la materia. Sin embargo, cabe destacar de la Directiva el cuadro amplísimo de excepciones que establece la Directiva, no para aquellos Estados cuya transferencia de datos tenga por objeto tratamiento informatizado o se destinen a ser objeto de tratamiento informatizado, entre países que “garanticen un nivel de protección adecuados” (art. 25-1), sino para aquellos países que no ofrecen dichos niveles adecuados de protección (art. 26), confirmándose con ello que cada día se impone “*la libre circulación de los datos*”⁽¹²⁴⁾ frente a los regímenes normativos que previeran excepciones de índole negativa al ejercicio del derecho de acceso a la información o datos personales contenidos

(124) Quizá lo más destacable de la Directiva sea precisamente la reglamentación, protección y garantía de uno de los principios-derechos más importantes del tratamiento informatizado, cual es, la “*libre circulación de los datos*”. Por ello, la Directiva 95/46/CE, en su epígrafe intitula: “...protección de las personas física en lo que respecta al tratamiento de datos personales y a la circulación de estos datos”. Es un principio programático presente en todo el procedimiento informatizado de datos personales y un derecho fundado en los derechos consecuentes del *habeas data* (derecho de acceso, rectificación, actualización y cancelación de datos o informaciones). Sobre este aspecto, la Directiva es insistente en los considerandos al exponer esta doble visión (principio-derecho) de la “*libre circulación de los datos*” (considerandos 3, 6, 8 y 9) y propugnar porque todo los Estados miembros de la UE, implementen todas las medidas jurídicas y técnicas (relativas a las nuevas tecnologías TIC e informática: software y hardware) necesarias para eliminar los obstáculos a la libre circulación, transferencia, y por ende acceso a los datos personales.

en ficheros o bancos de datos.

De esta forma, la Directiva establece reglas claras con respecto a las transferencias internacionales de datos: total libertad dentro de la Comunidad y prohibición (con ciertas excepciones, recogidas en el art. 26) cuando se trata de países terceros que no garanticen un nivel adecuado de protección ^[125]. Sin embargo, es lo cierto, que la mencionada prohibición frente al cúmulo de excepciones queda desvirtuada, pues tantas y de tal envergadura que bien puede afirmarse que el principio-derecho de *libre circulación de los datos* está garantizado tanto en la Comunidad como en el resto de Estados del mundo, sólo que estos últimos deben demostrar que se encuentran bajo el abrigo de una de las variopintas excepciones que veremos más adelante para España.

Aunque claro está, como especie de reserva normativa de carácter preventivo y en cierto modo de temor a una liberación total del principio-derecho de libre circulación de los datos para terceros países, se establece un criterio directriz para evaluar previamente el carácter de “*nivel adecuado de protección*” por parte de los Estados transmisores (emisor/receptor) de los datos personales.

En efecto, el carácter de nivel adecuado de protección se debe evaluar *a priori*, por el Estado involucrado, “atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencia de datos; en particular se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de derecho, generales o sectoriales, vigentes en el país tercero de que se trate, así como las normas profesionales y las medidas de seguridad en vigor en dichos países” (art. 25-2); es decir, analiza, evalúa y decide todas las circunstancias de modo, tiempo y lugar de la transferencia de datos personales: sí son datos personales generales o componentes del llamado *núcleo esencial de la privacidad*, y sobre todo, si existe normas idóneas de protección y seguridad en la transferencia de datos. Esta protección y seguridad últimas están rectamente dirigidas a las medidas necesarias que deben adoptar los Estados en la transferencia, tanto de tipo jurídico como tecnológico (soportes y medios de software y hardware).

Las excepciones en cascada, por niveles y rigurosamente condicionadas y previstas en el art. 26 de la Directiva 95/46/CE, tienen a proteger no a los Estados involucrados en la transferencia de datos personales, sino esencialmente al principio-derecho de la *libre circulación de datos*, que implica la protección y garantía de un grupo de derechos entre los que están los de *habeas data* y la *intimidación* (aunque indistintamente se use por la Directiva, “vida privada” o intimidad).

Se podrá transferir entre Estados, datos personales aún no teniendo uno de éstos niveles adecuados de protección, siempre y cuando: a) el interesado haya dado su consentimiento inequívoco a la transferencia, b) la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales tomadas a petición del interesado, c) la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar en interés del interesado, entre el responsable del tratamiento y un tercero, d) la transferencia sea necesaria o legalmente exigida para la salvaguardia de un interés público importante, o para el reconocimiento, ejercicio o de defensa de un derecho en un procedimiento judicial, e) la transferencia sea necesaria para la salvaguarda del interés vital del interesado, f) la transfe-

(125) Vid. DUMORTIER, J., y ALONSO BLAS, Diana M. *La transposición de la Directiva de protección...* Ob. cit. ut supra cit., pág. 11.

rencia tenga lugar desde un registro público, en virtud de disposiciones legales o reglamentarias, esté concebida para facilitar información al público y esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo, siempre que se cumplan, en cada caso particular, las condiciones que establece la ley para la consulta (art. 26-1).

También se podrá transferir datos personales a “un tercer país que no garantice un nivel de protección adecuado..., cuando el responsable del tratamiento ofrezca garantías suficientes respecto de la protección de la vida privada, de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los respectivos derechos; dichas garantías podrán derivarse, en particular, de cláusulas contractuales apropiadas” (art. 26-2).

Por su parte la LOPDP española de 1999, reglamenta la transferencia, circulación o comunicación de datos, en el artículo 33, como “Movimiento Internacional de datos”, de la siguiente manera:

1. No podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas.

2. El carácter adecuado del nivel de protección que ofrece el país de destino se evaluará por la Agencia de Protección de Datos (APD) atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de datos. En particular, se tomará en consideración la naturaleza de los datos de finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.

Se establece como excepciones al movimiento o flujo de datos, las siguientes: (i) Cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que sea parte España; (ii) Cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional; (iii) Cuando la transferencia sea necesaria para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamiento médicos o la gestión de servicios sanitarios; (iv) Cuando se refiera a transferencias dinerarias conforme a su legislación específica; (v) Cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista; (vi) Cuando la transferencia sea necesaria para la ejecución de un contrato entre el afectado y el responsable del fichero o para la adopción de medidas precontractuales adoptadas a petición del afectado; (vii) Cuando la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar, en interés del afectado, por el responsable del fichero y un tercero; (viii) Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público. Tendrá esta consideración la transferencia solicitada por una Administración fiscal o aduanera para el cumplimiento de sus competencias; (ix) Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial; (x) Cuando la transferencia se efectúe, a petición de persona con interés legítimo, desde un Registro Público y aquélla sea acorde con la finalidad del mismo; y (xi) Cuando la transferencia tenga como destino un Estado miembro de la Unión Europea, o un Estado respecto del cual la Comisión de

las Comunidades Europeas, en el ejercicio de sus competencias, haya declarado que garantiza un nivel de protección adecuado.

3.3.4.2. En el ámbito del derecho colombiano

En el Proyecto de Ley Estatutaria No. 221/2007 de Cámara y No. 027/2006 de Senado, acumulado con el No. 05/2006 Senado, se hace referencia a la circulación de la información para referirse al aspecto tratado en normas internacionales como movimiento o transferencia de datos.

Como decíamos anteriormente "*La autodeterminación informática es la facultad de la persona a la cual se refieren los datos, para autorizar su conservación, uso y circulación...*" (SU-082-1995), las facultades que hacen parte del núcleo esencial del Hábeas data, previstas en el inciso 2º del artículo 15, constitucional.

El proyecto de ley estatutaria, siguiendo muy de cerca en este punto a la sentencia T-729-2002, regula la circulación de datos o informaciones personales invirtiendo la regla general del derecho europeo y español, es decir, restringiendo la circulación de la información, salvo algunas excepciones, cuando en el derecho europeo y español como hemos visto la regla es la libre circulación de los datos personales, con un régimen amplio de excepciones, como pudimos examinar anteriormente.

El artículo 1º del proyecto de ley al presentar su objeto lo presenta como una forma de desarrollar el derecho que tiene toda persona a conocer, actualizar y rectificar las informaciones que se hayan recabado en bancos de datos; así mismo los derechos y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales y finalmente el derecho a la información.

En el cuadro de la principialística de la administración de los datos, puntualmente tratada por la Corte Constitucional en la Sentencia T-729-2002, el proyecto de ley se refiere a la circulación de datos en el artículo 4º literales a, c y g, es decir, en los principios de veracidad o calidad de los registros o datos, circulación restringida y confidencialidad. El primero, porque se "*prohíbe el registro y divulgación de datos parciales, incompletos, fraccionados o que induzcan a error*"; el tercero cuando expresa que "*todas las personas naturales o jurídicas que intervengan en la administración de datos personales que no tengan la naturaleza de públicos están obligadas en todo tiempo a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende la administración de datos, pudiendo sólo realizar suministro o comunicación de datos cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma*".

El principio de la circulación restringida específico en lo que atañe a la comunicación de datos, manifiesta: "*La administración de datos personales se sujeta a los límites que se derivan de la naturaleza de los datos, de las disposiciones de la presente ley y de los principios de la administración de datos personales especialmente de los principios de temporalidad de la información y la finalidad del banco de datos*". Y agrega en el inciso 2º: "*Los datos personales, salvo la información pública, no podrán ser accesibles por Internet o por otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los titulares o los usuarios autorizados conforme a la presente ley*".

La primera parte del principio es una remisión normativa interna a otros principios como el de temporalidad y finalidad de los datos, pero sobre la circulación, transferencia,

movimiento o comunicación de datos la norma solo atina a decir que se sujetará a los límites que se derivan de la naturaleza de los datos, pero en realidad de verdad no es expresivo ni comprensible de lo que se debe entender básicamente como circulación de datos por medios tradicionales, tecnológicos (teléfono, fax, radiotransmisión, etc.) o medios electrónicos, informáticos o telemáticos (Computador, red de redes de información, o por medios TIC), tanto a nivel interno o nacional entre entidades, organismos o dependencias del Estado o personas privadas con función pública o particulares, como a nivel internacional con entidades estatales o particulares, siempre y cuando se cuente con niveles de seguridad tecnológica y jurídicas apropiadas. La segunda parte de la norma se limita a la prohibición de la circulación de datos, salvo los casos autorizados por la ley y los titulares.

La Corte Constitucional en sentencia T-729-2002, con el mismo sentido restrictivo del principio plasmado en el proyecto de ley, se pronuncia cuando sostiene: “*el principio de circulación restringida, estrechamente ligado al de finalidad, la divulgación y circulación de la información está sometida a los límites específicos determinados por el objeto de la base de datos*”, con lo cual antes de poner en circulación o movimiento un dato personal, primero deberá averiguarse cuál es el objeto y la finalidad del banco de datos en donde se haya recabado el dato y consecuentemente si se dispone o no del consentimiento del titular de los datos.

Así mismo, al referirse a los deberes de los operadores de los bancos de datos, el proyecto de ley estipula que éstos deberán “*Garantizar, que en la recolección, tratamiento y circulación de datos, se respetarán los demás derechos consagrados en la ley*” (Artículo 7-2). En este aspecto el proyecto de ley acierta pues es una garantía de toda persona que los responsables de los bancos de datos o centrales de información financiera o especializada al tratar, procesar o más aún comunicar datos deben garantizar la no amenaza o vulneración de los derechos fundamentales y particularmente el de la intimidad, el buen nombre, el honor, el Hábeas data y el de información.

Finalmente, el proyecto de ley se refiere en concreto al fenómeno de la circulación de datos o informaciones en el artículo 5º, el cual manifiesta:

La información personal recolectada o suministrada de conformidad con lo dispuesto en la ley a los operadores que haga parte del banco de datos que administra, podrá ser entregada de manera verbal, escrita, o puesta a disposición de las siguientes personas y en los siguientes términos: (i) A los titulares, a las personas debidamente autorizadas por estos y a sus causahabientes mediante el procedimiento de consulta previsto en la presente ley; (ii) A los usuarios de la información, dentro de los parámetros de la presente ley; (iii) A cualquier autoridad judicial, previa orden judicial; (iv) A las entidades públicas del poder ejecutivo, cuando el conocimiento de dicha información corresponda directamente al cumplimiento de alguna de sus funciones; (v) A los órganos de control y demás dependencias de investigación disciplinaria, fiscal, o administrativa, cuando la información sea necesaria para el desarrollo de una investigación en curso; (vi) A otros operadores de datos, cuando se cuente con autorización del titular, o cuando sin ser necesaria la autorización del titular el banco de datos de destino tenga la misma finalidad o una finalidad que comprenda la que tiene el operador que entrega los datos. Si el receptor de la información fuere un banco de datos extranjero, la entrega sin autorización del titular sólo podrá realizarse dejando constancia escrita de la entrega de la información y previa verificación por parte del operador de que las leyes del país respectivo o el receptor otorgan garantías suficientes para la protección de los derechos del titular.

El principio de circulación restringida en nuestro país, según el proyecto de ley regula el movimiento o circulación de datos o informaciones desde el punto de vista pasivo, es decir, desde la entidad, organismo o dependencia del estado nacional o desde las personas o entidades de carácter particular nacional o extranjero (tan solo del sector financiero) a quienes se entrega la información, la cual parece sugerir el proyecto de ley sólo es de carácter tradicional o documental escrita y no informatizada o sometida a tratamiento informático por medios electrónicos o telemáticos. Esta duda surge porque al comienzo de la norma se dice que la información se entregará “de manera verbal, escrito o puesta a disposición...”

La Comunicación o circulación de datos que incluye un fenómeno de información en doble vía: emisor (mensaje-Feed back-retroalimentación) receptor ^[126], parece no estar presente en el principio de circulación restringida, pues sólo se obliga quien entrega la información y no existen los niveles de protección de la información que el derecho europeo, español e incluso el Argentino manejan a través de las excepciones a la regla general de la libre circulación de los datos personales.

La Ley 1266 de 2008, recoge los principios universales de tratamiento, administración y transmisión, flujo o circulación de los datos, bajo el criterio de los principios que orientan la administración de los datos, la prohibición y restricción de la transmisión de algunos datos personales y como norma especial para compatibilizar el llamado “flujo internacional de datos” con terceros países, que tanto requieren los Estados Modernos para entablar medidas de seguridad y confianza sobre los datos personales (dentro de ellos, la especie de “datos financieros”) transnacionales.

En efecto, es un principio de la administración de los datos, “*la circulación restringida de los datos*”, prevista en el artículo 4º, literal c) de la Ley citada.

Este consiste en que “*La administración de datos personales se sujeta a los límites que se derivan de la naturaleza de los datos, de las disposiciones de la presente ley y de los principios de la administración de datos personales especialmente de los principios de temporalidad de la información y la finalidad del banco de datos.*”

Los datos personales, salvo la información pública, no podrán ser accesibles por Internet o por otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los titulares o los usuarios autorizados conforme a la presente ley”.

La circulación de los datos, prevista en el artículo 5º de la Ley mentada, la expone así: “*La información personal recolectada o suministrada de conformidad con lo dispuesto en la ley a los operadores que haga parte del banco de datos que administra, podrá ser entregada de manera verbal, escrita, o puesta a disposición de las siguientes personas y en los siguientes términos: a) A los titulares, a las personas debidamente autorizadas por estos y a sus causahabientes mediante el procedimiento de consulta previsto en la presente ley; b) A los usuarios de la información, dentro de los parámetros de la presente ley; c) A cualquier autoridad judicial, previa orden judicial; d) A las entidades públicas del poder ejecutivo, cuando el conocimiento de dicha información corresponda directamente al cumplimiento de alguna de sus funciones”* ^[126 bis].

(126) RIASCOS GOMEZ, Libardo. **La Constitución de 1991...** Ob.,ut supra cit. p. 3

(126 bis) Declarado exequible condicionalmente, mediante Sentencia C-1011-2008, “en el entendido que..., las entidades públicas del poder ejecutivo, cuando acceden al dato personal, quedan sometidas a los deberes y responsabilidades previstos por la Ley Estatutaria para los usuarios de la información”.

BILIOGRAFIA GENERAL

AA.VV. ***Colección de discos compactos de Aranzadi***. Ed. Aranzadi, Pamplona, 1997.

AA.VV. ***Constituição Novo Texto***. Coimbra editora, Edição organizado JJ. Gomes Conotilho o vital M., 1982

AA.VV. ***Documentación Informática***. Serie Amarilla. Tratados Internacionales núm. 2.

AA.VV. ***Exposición de Motivos del Proyecto de Ley Estatutaria No. 64 de 2003***.

AA.VV. ***Exposición de Motivos del Proyecto de Ley Estatutaria de 2005***. Vía Internet.

AA.VV. ***El Hábeas Data en el Derecho Venezolano***. En: <http://www.conhist.org/>

AA.VV. ***El proceso de Hábeas data en la Región Andina***. En: www.caipe.org.pe/

AA.VV. ***La acción de hábeas data***. DDG-167-01/ 16-07-2001. En: <http://www.defensoria.gov.ve/>

AA.VV. ***Ley sobre protección a la vida privada o protección de datos de carácter personal***. En: <http://www.sernac.cl/leyes/>

BARDELLII LARTIRIGOYEN, Juan B. ***El derecho de Hábeas Data en el Código Procesal constitucional y en la jurisprudencia del tribunal Constitucional***. En: <http://www.riaj.org/>

BARZALLO, José Luís. ***Presidente AEDIT***. Blog del Foro de Hábeas Data. En: ***Ecuador: Ley de Protección de Datos***. Mayo 30 de 2006.

BAIGORRI, Mauricio Javier et all. ***La Naturaleza jurídica del Hábeas Data***. En: <http://www.salvador.edu.ar>

BAZAN, Víctor. ***Revista Semestral del Centro de Estudios constitucionales***. Universidad de Talca, Facultad de ciencias jurídicas, Santiago de Chile. En: www.librotecnia.cl

BENITEZ, Luis María. ***Análisis comparativo entre Hábeas Data y acción de amparo en Paraguay***. Revista Ius et Praxis, No. 3º, Número 1, Facultad de Ciencias Jurídicas y Sociales, Universidad de Talca, Talca (Chile).

CASTELLS ARTECHE, José M. **La Intimidad informática**. En: Estudios sobre la Constitución Española en homenaje al profesor Eduardo García de Enterría. Ed. Civitas, Tomo II, Madrid, 1991.

CARRANZA TORRES, Luis. **El sistema de protección de datos en Córdoba**. En: <http://www.informatica-juridica.com>.

CHANAME ORBE, Raúl. **Hábeas Data y el Derecho fundamental a la intimidad de la persona**. En: <http://www.sisbib.unmsm.edu.pe>

CIFUENTES MUÑOZ, Eduardo. **El Hábeas Data en Colombia**. Revista Ius et Praxis, Año 3, Número 1º, Facultad de ciencias jurídicas y sociales, Universidad de TALCA, Talca (Chile), 1997.

DA SILVA, José Alfonso. **Curso de derecho constitucional positivo**. En: www.astrea.com.ar

DE ABREU DALLARI, Dalmo. **Disertación pronunciada en el Seminario Iberoamericano sobre la Acción de "Hábeas Data"**. Citado por PUCCINELLI, Oscar. Hábeas Data en el Brasil. En: <http://www.astrea.com.ar>

DE LA SERNA BILBAO, María Nieves. **La agencia de protección de datos española: con especial referencia a su característica de independencia**. En: Actualidad Informática Aranzadi. Ed. Aranzadi, S.A., Núm. 22 de Enero, Pamplona, 1997.

DUBIE, Pedro. **El Hábeas Data financiero**. Revista de Derecho Informático. ISS 1681-5726. Ed. Alfa-Redi, No. 038, Septiembre de 2001

DUMORTIER, J., y ALONSO BLAS, Diana M. **La Transposición de la Directiva de protección de datos en Bélgica**. En: Actualidad Informática Aranzadi. Ed. Aranzadi, S.A., Núm. 20 de Julio, Pamplona, 1997

DURAN RIBERA, Willman R. **Contenido y alcances del Hábeas Data en Bolivia**. En: <http://www.tribunalconstitucional.gov.bo/>

EQUIGUREN, Francisco. **El Hábeas Data y su desarrollo en el Perú**. Revista Ius et Praxis, Año 3, Número 1º, Facultad de ciencias jurídicas y sociales, Universidad de Talca, Talca (Chile).

FAIREN GUILLEN, Víctor. **El Hábeas Data y su protección actual surgida en la Ley española de Informática del 29 de Octubre (Interdictos, Hábeas Corpus) –Primera Parte—** En: Revista de Derecho procesal. R.D.P. No. 3º, Madrid, 1996

FLOREZ DAPKEIVICIUS, Rubén. **Protección de Datos Personales de Informes Comerciales: Ley 17838 de Uruguay.** Invitado en el WEB: El Derecho Público Mínimo. En: <http://www.udenar.edu.co/derechopublico>

GARCIA BELAUNDE, Domingo. **Diferencias entre el Hábeas Data y la Acción de amparo o tutela constitucional en Perú.** Revista Ius et Práxis, Año 3, Número 1, Facultad de ciencias jurídicas y sociales de Talca, Talca (Chile), 1997.

GARCIA BERNI, Aída. **La acción de Hábeas Data. Asesora del Tribunal Constitucional.**

GIGLI, Juan. **Venezuela: Quinta jornada pública de la Ley de Tecnología de la Información.** Enviado Vía Internet. Mayo 8 de 2006

GORDILLO T. José F. y RESTREPO, Yepes. **Introducción al análisis del derecho fundamental del hábeas data.** En: <http://www.urosario.edu.co>

GOZAINI, Osvaldo A. **El Proceso de Hábeas Data en la Nueva Ley (de protección de datos Argentina).** Vía Internet.

HERNANDEZ, Jaime A. y VARGAS, Javier. **Ponencia para primer debate al proyecto de Ley Estatutaria 201 de 2003, Cámara y O71 de 2002, Senado.** Vía Internet.

H., Benjamín Miguel. **Acción de amparo relacionada con la protección de datos persona les en el orden jurídico boliviano.** Revista Ius et Praxis, Año 3, Número 1º, Facultad de Ciencias jurídicas y sociales, Universidad de Talca, Talca (Chile), 1998.

KATSH, Ethain. **Rights, Camera, Action: Cyberspatial settings and the first amendment.** Professor of Legal Studies, University of Massachusetts at Amherst; B.A. 1967, New York University; J.D. 1970, Yale University. En: www.umontreal.edu.ca.

LAMA MORE, Héctor Enrique. **El Hábeas Data en el Perú. El Estado de cosas inconstitucional en el caso Arellano Serquen contra el CNM.** Vía Internet.

LIVELLARA, Silvana. **Hábeas Data e informática crediticia. La Eventual responsabilidad civil de las entidades financieras y del Banco Central de la República Argentina por cesión y publicidad de datos inexactos.**

LOPEZ MARTINEZ, Juan. **La protección de los datos y la información en poder de la Hacienda Pública.** Profesor de Derecho financiero y tributario. Vía Internet, 2007.

MARIN GARCIA, Gustavo J. ***Evolución de la protección del derecho al acceso y control de la información en la jurisprudencia de Venezuela.*** En: <http://www.informatica-juridica.com/trabajos/>

MARTELLA, Lilián, ***Hábeas Data: Garantía de una Dimensión fundamental de la libertad.*** En: <http://www.ceride.gov.ar/>

MIRABELLI, ***“Banche dati e contemperamento degli interessi”***, *Banche dati telematica e diritti della persona*, Cedam, Padova, 1984, pág. 160. Citado por ORTI V. Ob. cit., p. 11

MOEYKENS, Federico Rafael. ***Derecho a la libertad informática: consecuencias del Habeas Data.*** Revista de Derecho Informático. Alfa-Redi No. 046, Mayo de 2002. Vía Internet.

NOGUERA ALCALA, Humberto. ***Reflexiones sobre el establecimiento constitucional del Hábeas Data y del proyecto en tramitación parlamentaria sobre la materia.*** Revista *Ius et Praxis*, Número 1º, Facultad de ciencias jurídicas. Universidad de Talca, Talca (Chile), 1997

NUÑEZ PONCE, Julio. ***La Acción Constitucional de Habeas Data y la Comercialización de Información Judicial en Internet.*** Revista de Derecho Informático. ISSN 1681-5726, Edita: Alfa-Redi No. 013 - Agosto del 1999. En: <http://www.alfa-redi.org>

PALAZZI, Pablo. ***El Hábeas Data en el derecho Argentino.*** Revista de Derecho Informático. ISSN 1681-5726, Edita: Alfa-Redi No. 004 - Noviembre del 1998. En: <http://www.alfa-redi.org>

PEREZ, Efraín y MAKOWIAK, Jéssica. ***El derecho de acceso a la información en Europa y América Latina: un enfoque constitucional.*** En: <http://www.cica.es>

PEREZ LUÑO, Enrique. ***Derechos Humanos, Estado de Derecho y Constitución.*** Ed. Tecnos, S.A., Madrid, 1984, p. 359 y ss.

PINTO FERREIRA, Luiz. ***Os instrumentos processuais protetores dos direitos no Brasil.*** En la obra colectiva: *Jurisdicción constitucional en Iberoamérica*

PUCCINELLI, Oscar. ***Tipos y subtipos de Hábeas Data en América Latina.*** Ed. Astrea, Buenos Aires (Argentina). En: www.astrea.com

_____ ***El “Hábeas Data” en Brasil.*** En: www.astrea.com.ar

QUIROGA LAVIÉ, Humberto. ***El amparo, el hábeas data y el hábeas corpus en la reforma de la constitución – Explicada por miembros de la comisión de redacción.*** Rubinzal Culzoni. Santa Fe. 1994

REMOLINA ANGARITA, Nelson. ***Del Actual proyecto de Ley Estatutaria del Hábeas Data en Colombia.*** En: www.gecti.org.co

_____ ***Documentos GECTI sobre el hábeas Data y la protección de datos personales.*** En: www.gecti.org.co

_____ ***Del actual proyecto (No. 071 de 2002) de Ley estatutaria del Hábeas Data en Colombia.*** Facultad de Derecho de la Universidad de los Andes. nremolin@uniandes.edu.co

_____ ***Censos, estadísticas y datos personales en la era del gobierno electrónico.*** Universidad de los Andes, Facultad de Derecho, Abril de 2005. En: <http://gecti.uniandes.edu.co/>

RIASCOS GOMEZ, Libardo O. ***El derecho a la intimidad, la visión iusinformativa y el delito de los datos personales.*** Tesis Doctoral, Universidad de Lleida (España), Lleida, 1999, p. 336-371.

_____ ***“Los datos personales de carácter económico o financiero en el proyecto de habeas data de 2002”.*** En: www.udenar.edu.co/derechopublico

_____ ***La Constitución de 1991 y la Informática Jurídica.*** Ed. UNED, Universidad de Nariño, Pasto, 1997

_____ ***Los datos personales de carácter financiero en los proyectos de ley estatutaria de Hábeas Data de origen parlamentario y gubernamental en Colombia.*** Ensayo jurídico para la Revista Electrónica Española de Derecom, Universidad de Valladolid (España). Vía Internet En: www.derecom.com.es

_____ ***Las medidas cautelares en el procedimiento administrativo.*** Tesis Doctoral, Universidad de Navarra, Pamplona (España), 1986.

_____ ***Los actos y el procedimiento administrativo en el derecho colombiano.*** Ed. Castellana, Pasto, 2001

RYSDALL, R. ***Protección de datos y el Convenio Europeo de los derechos humanos.*** Novática, Marzo de 1992. Citado por AA.VV. ***Revista de Ciencias Jurídicas,*** Facultad de derecho, Universidad de Costa Rica, No. 103, Costa Rica, 2003

SAGUES, Néstor Pedro. ***El Hábeas Data en Argentina (Orden Nacional).*** Revista Ius et Práxis, Facultad de ciencias jurídicas y sociales, Universidad de Talca (Chile), Chile, 1997

SORIN, Sergio. ***El Hábeas Data en Argentina: Invasión de la privacidad.*** Buenos Aires, Marzo 21 de 2000.

SOUVIRON, José M. **En torno a la juridificación del poder informático del Estado.** R.V.A.P. Núm. 40, Sep-Dic., Bilbao, 1994

SOUMINEN, Kati. **Acceso a la información en América Latina y del Caribe.** Universidad de California, San Diego. En: <http://www.thedialogue.org/publications>

TANUS, Gustavo Daniel. **Protección de datos personales, principios generales, derechos, deberes y obligaciones.** En: <http://www.protecciondedatos.com.ar>

TORRES CASTRO, Carlos A. **Código Procesal Constitucional.** Estudio preliminar, 1ª ed., Sociedad de Estudios para una cultura de paz, Lima (Perú), Noviembre 30 de 2004.

URIOSTE, Mercedes. **Protección de datos personales.** En: <http://www.derecho-comparado.com>

VAN DER MENSBRUGGHE, Patricia. En: **Flujos transfronterizos de datos en la Directiva 95/46 de las Comunidades Europeas.** En: Revista Actualidad informática Aranzadi. Ed. Aranzadi S.A., No. 20 Julio, Elcano (Navarra), Madrid, 1996

VILLAVECES HOLLMAN, Juan M. **Reflexiones en torno a la necesidad de un marco regulatorio sobre el Hábeas Data.** Foro Universidad de los Andes, Noviembre 18 de 2003, Bogotá, 2003