

EL HÁBEAS DATA Y EL DERECHO DE AUTODETERMINACIÓN INFORMATIVA EN PERSPECTIVA DE DERECHO COMPARADO^(*)

Victor Bazán^(**)

Sumario: INTRODUCCION. I. CONSIDERACIONES PREVIAS. II. ACERCAMIENTO CONCEPTUAL AL HÁBEAS DATA. III. UN RECORRIDO POR EL DERECHO COMPARADO. IV. SOBRE ALGUNOS LINEAMIENTOS BÁSICOS QUE DEBERÍAN SER TENIDOS EN CUENTA POR LAS FUTURAS REGULACIONES QUE EN LA REGIÓN IBEROAMERICANA SE DICTEN EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES. V. ANÁLISIS PARTICULARIZADO DEL DERECHO DE AUTODETERMINACIÓN INFORMATIVA. EPÍLOGO.

INTRODUCCIÓN

Esbozado en breves líneas, el presente comenzará con un enfoque introductorio donde se pondrá de manifiesto la necesidad de que el Derecho ofrezca en general respuestas adecuadas frente a los nuevos desafíos tecnológicos y, en particular, de cara a la necesaria protección de los datos personales (*rectius*: de la persona que ostenta la titularidad de los mismos) ante los novedosos retos que plantea el incesante desarrollo informático.

En ese camino, delinearemos a continuación algunas pautas liminares para conceputar y perfilar la figura del hábeas data; luego, recorreremos distintas soluciones que, para operativizar dicha protección de los datos personales, proporciona el derecho comparado, tanto internacional como nacional, y, dentro de este último, sus vertientes constitucional, infraconstitucional y jurisprudencial.

Posteriormente, y previo a brindar las observaciones finales que clausurarán el trabajo, nos detendremos a analizar el bien jurídico que subyace en la protección de los datos personales y el hábeas data, en torno de lo cual, y frente a la insuficiencia jurídica del concepto preinformático de la intimidad, sostendremos argumentalmente que tal rol debe ser cumplido por el derecho de autodeterminación informativa, que tiene una naturaleza autónoma y que exhibe una dimensión bifocal: sustancial y, a su vez, instrumental de otros derechos.

Todo ello, en el entendido de que debe dotarse a la persona de suficientes facultades de control sobre el cúmulo de información que sobre ella circula, contralor que debe operar no sólo durante el almacenamiento de aquélla sino también en toda la extensión del proceso encaminado a obtenerla.

^(*) Agradecemos profundamente a los responsables de la *Revista de Derecho Constitucional*, profesores LUIS A. ORTIZ-ÁLVAREZ, JACQUELINE LEJARZA y JOSÉ VICENTE HARO por permitirnos participar –una vez más– de la valiosa publicación que dirigen.

^(**) Profesor Titular Efectivo de Derecho Constitucional de la Facultad de Derecho y Ciencias Sociales de la Universidad Católica de Cuyo (San Juan, Argentina). Profesor de Cursos Intensivos de Postgrado en la Universidad de Buenos Aires (Argentina). Miembro Titular e integrante del Comité Ejecutivo de la Asociación Argentina de Derecho Constitucional. Miembro Titular de la Asociación Argentina de Derecho Procesal.

I. CONSIDERACIONES PREVIAS

Comenzamos estas líneas introductorias con un interrogante: ¿Puede el Derecho permanecer inmóvil frente a los incesantes cambios tecnológicos? Definitivamente, no.

Los innumerables avances que genera la evolución tecnológica plantean nuevos desafíos respecto de los que el Derecho “debe” hacerse cargo. Y, particularmente con relación a la informática, es incuestionable que el tratamiento masivo de la información y su innegable connotación crematística expanden sus efectos, ingresando en la superficie propia de los derechos fundamentales, por lo que –sin duda– deberán brindarse adecuadas respuestas jurídicas para conferir protección al ser humano¹.

En forma acertada se ha sostenido que la utilización de los datos personales, en virtud de su rentabilidad comercial y –lo que puede resultar más peligroso– su empleo con fines de contralor político sobre las actividades privadas, han dejado al descubierto la contracara de una importante conquista tecnológica cuya adecuada funcionalidad exige límites jurídicos².

No nos inspira el misonéismo. Por el contrario, nuestro aporte intenta ubicarse –dentro de parámetros realistas– en una senda que se dirija hacia el equilibrio de los valores en juego; contexto en el que advertimos la presencia del hábeas data como importante arma defensiva dispensada al individuo para activar su derecho de autodeterminación informativa –punto nuclear de este trabajo– y tutelar, de tal modo, sus datos personales frente a la potencialidad nociva de, v.gr., un flujo cibernético indiscriminado de información.

En el marco anunciado, debemos reconocer que la evolución cuantitativa y cualitativa de las investigaciones, conquistas tecnológicas, etc., puede tener una incidencia muy profunda en la médula misma del sistema jurídico, existiendo –fundamentalmente en el caso de la informática– el riesgo cierto de que la inagotable sofisticación conduzca a vulnerar fundamentales derechos de la persona (a la privacidad, igualdad, libertad religiosa –*inter alia*–).

La sociedad informatizada afronta nuevos riesgos y el Derecho “debe” estar a la altura de las circunstancias. No se trata de plantear la cuestión en términos de una lucha entre la sociedad cibernética y los derechos fundamentales. Juzgamos superada la etapa en que el problema discurría como una tensión dialéctica entre “vida privada vs. computadoras”, pues el presente estadio de la evolución de la normativa tuitiva de la información personal constituye una síntesis de los intereses sociales e individuales en juego³.

Allí se aloja el nudo del problema: en la necesidad de buscar una equitativa conciliación de tales valores. Por una parte, el interés público encarnado en el accionar estatal en el sentido de acopiar, de reunir información acerca de las personas

¹ Y, por qué no, también a la persona moral o de existencia ideal.

² Cfr. MARCHENA GÓMEZ, MANUEL, “Intimidad e Informática: La protección jurisdiccional del hábeas data”, *Boletín de Información*, Ministerio de Justicia, N° 1.768, Madrid, España, 15 de febrero de 1996, p. 746.

³ BATTO, HILDA, “Informática, Libertad y Derechos Humanos”, en *Derecho Informático*, Edit. Depalma, Buenos Aires, Argentina, 1987, p. 249; cit. por TRAVIESO, JUAN ANTONIO, *Derechos Humanos y Derecho Internacional*, Edit. Heliasta S.R.L., Buenos Aires, Argentina, 1990, p. 354.

que viven en su territorio (o el de particulares que, cumpliendo una actividad lícita, almacenen datos y lucren con la prestación del servicio de brindar información crediticia, solvencia patrimonial, etc.) y, por otro lado, el interés propio de los individuos (titulares de los datos registrados) de buscar protección para sus derechos fundamentales, intentando hacerlos valer en los casos concretos de vulneración de ellos, o bien, previniendo que tales perjuicios se corporicen. En conexión con ello, SAGÜÉS⁴ sostiene que el hábeas data fue concebido para brindar una respuesta de tipo transaccional entre los intereses de registrantes y de registrados.

La cuestión medular que abordamos no estriba en el uso informático; la dificultad aparece cuando dicho *uso informático* se convierte en *abuso informático*. Precisamente, la idea es que éste sea evitado o prevenido; o, para el caso de no poder serlo, que se proporcionen herramientas adecuadas para la protección de los derechos individuales y restablecer, así, el equilibrio que se hubiere quebrado.

En el marco descripto enraíza la razón de ser del mentado hábeas data, que surge como un muro de contención para evitar o frenar el abuso informático o de captación, almacenamiento y uso antijurídicos de información por otros medios o soportes.

Debe quedar en claro que la implementación del hábeas data en modo alguno debiera procurar inhibir la recopilación de datos para fines investigativos, científicos o periodísticos ni el acopio de información para cumplir objetivos estadísticos.

Lo que en realidad se pretende proscribir es que esa información sea usada ilícita o disfuncionalmente, que se abuse de la misma y que con ello se provoquen un perjuicio a su titular.

Ya para concluir esta referencia introductoria, cabe señalar que, paralelamente, se procura evitar los efectos de la perniciosa *inferential relation retrieval*, que consiste en la descontextualización de la información a través del “cruce” de datos veraces con otras referencias de signo distinto, lo que arroja como precipitado una información no cabal⁵, caso en el que —como se ha señalado— la agresión a la autodeterminación informativa se origina, no ya porque se produzca una apropiación incontrolada de los mismos, “sino porque se instrumentalizan los disponibles para fabricar una personalidad y sustituir la propia identidad por otra que no tiene por qué corresponderse con la verdadera”⁶.

II. ACERCAMIENTO CONCEPTUAL AL HÁBEAS DATA⁷

Según las particularidades léxico-jurídicas del país de que se trate, puede conceputarse al hábeas data como una acción, una garantía constitucional, un procedi-

⁴ SAGÜÉS, NÉSTOR P. “Amparo, hábeas data y hábeas corpus en la reforma constitucional”, *La Ley*, Buenos Aires, Argentina, 7 de octubre de 1994, p. 3.

⁵ Cfr. LUCAS MURILLO DE LA CUEVA, PABLO, *El derecho a la autodeterminación informativa*, Tecnos, Madrid, España, 1990, p. 111.

⁶ LUCAS MURILLO DE LA CUEVA, PABLO, “Informática y protección de datos personales”, *Cuadernos y Debates*, N° 43, Centro de Estudios Constitucionales, Madrid, España, 1993, p. 83.

⁷ A modo de advertencia liminar, adelantamos que sólo se enfocará lo que algunos autores denominan como “*hábeas data propio o tradicional*”, es decir, el destinado a la instrumentación protectoria de los datos personales, que en puridad constituye la verdadera génesis de la figura; por tanto, no abordaremos el “*hábeas data impropio*”, el que —según los seguidores de tal escisión taxonómica— tutela el derecho de los habitantes al acceso a la información pública.

miento jurisdiccional de trámite especial y sumarísimo, un proceso constitucional o un recurso protectorio del derecho de autodeterminación informativa o derecho a la protección de los datos personales, frente a los posibles excesos del poder de registración precisamente de la información de carácter personal.

En otras palabras, a través del hábeas data el legitimado (persona física o jurídica) puede acceder al conocimiento de sus datos personales y los referidos a sus bienes y al destino de tal información que se encuentren asentados en archivos, registros, bancos de datos u otros medios técnicos, electrónicos y ópticos, de carácter público o privado, de soporte, procesamiento y provisión de la información; y, en determinadas hipótesis (por ejemplo, falsedad o uso discriminatorio de tales datos), exigir la supresión, rectificación, actualización o el sometimiento a confidencialidad de los mismos.

La expresión 'hábeas data' es utilizada a modo de empréstito terminológico de la de 'hábeas corpus'. Recordamos que ésta última significa que "se tenga, traiga, exhiba o presente el cuerpo (ante el juez)", mientras que en el caso del 'hábeas data' se quiere connotar "que se tenga, traiga, exhiba o presente los datos". La locución 'hábeas data' se forma con *habeas* (del latín *habeo*, *habere*), que significa tener, exhibir, tomar, traer, etc.; adosándole el vocablo *data*, respecto del cual existe alguna disputa léxica, pues mientras algunos afirman que se refiere al acusativo neutro plural de *datum*: lo que se da, datos –también del latín–; otros sostienen que la palabra *data* proviene del inglés, con el significado de información o datos⁸.

III. UN RECORRIDO POR EL DERECHO COMPARADO

La problemática relativa al derecho a la protección de los datos personales ha sido abordada en diversos instrumentos internacionales tanto de Naciones Unidas (ONU) y del Consejo de Europa, como de otras organizaciones internacionales; también, en la propia Unión Europea. Además, ha quedado plasmada como preocupación constitucional y legislativa en numerosos países de Europa y de América. Tal panorama normativo será repasado sucintamente a continuación.

1. En el ámbito internacional

A. En el marco *universal*, puede contabilizarse la Resolución 45/95 de la Asamblea General de la ONU, de 14 de diciembre de 1990, en la que se recoge la versión revisada de los 'Principios rectores aplicables a los ficheros computarizados de datos personales'.

Asimismo, en la Organización de Cooperación y Desarrollo Económicos (OCDE), deben ser tenidas en cuenta: la Recomendación relativa a las directrices aplicables a la protección de la vida privada y a los flujos transfronterizos de datos personales, adoptada por el Consejo de la OCDE el 23 de setiembre de 1980; la

⁸ Por nuestra parte, añadimos que en traducción literal, *data* significa la "información conocida antes de comenzar a solucionar un problema". Originalmente *data* era el plural y *datum*, el singular; actualmente *data* se emplea invariablemente para el singular y el plural –dato o datos– (cfr. CARVER, WALLACE y CAMERON, *Collins English Learner's Dictionary*, Gran Bretaña, 1974, p. 129). Se define la palabra *data*, también, como "la información organizada, generalmente utilizada como base de una decisión"; y, en su sentido corriente, como "información organizada, recabada para un propósito específico" (cfr. BLACK, *Black's Law Dictionary*, 5ª ed., St. Paul Minn., West Publishing Co., EE.UU., 1979, p. 356).

Declaración relativa a los flujos transfronterizos de datos no personales, adoptada por los Gobiernos de los Países Miembros de la OCDE el 11 de abril de 1985; la Recomendación relativa a las directrices de política criptográfica, adoptada por el Consejo de la OCDE el 2 de marzo de 1997; y la Declaración relativa a la protección de la intimidad en las redes globales, realizada por los Ministros de la OCDE en la conferencia “Un mundo sin fronteras: comprender el potencial del comercio electrónico global”, celebrada entre el 7 y el 9 de octubre de 1998 en Ottawa, Canadá.

B. Ya en la órbita del *Consejo de Europa*, brilla con luz propia el ‘Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal’, adoptado en 1981 en Estrasburgo, y que entrara en vigor el 1 de octubre de 1985. Tal Convenio procura –como se expresa en su Preámbulo– “conciliar los valores fundamentales del respeto a la vida privada y de la libre circulación de la información entre los pueblos”, y su marco de aplicación se circunscribe a los ficheros y a los tratamientos automatizados de datos de carácter personal, en los sectores público y privado (art. 3.1)⁹.

C. En el plano del derecho comunitario europeo, emerge como instrumento de gran importancia la Directiva 95/46/CE de 25 de octubre de 1995, del Parlamento Europeo y el Consejo¹⁰. Tal Directiva se refiere a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de éstos, y a la misma debían quedar ajustadas (al 25 de octubre de 1998) las preceptivas internas de los Estados componentes de la Unión Europea, lo que provocó un intenso movimiento legislativo en tal sentido. Ello, con el objeto de eliminar la disparidad que entre tales normativas legales surgía en relación con los niveles de protección de los datos, circunstancia que podría funcionar como óbice para la transmisión de información entre dichos Estados¹¹.

Por su parte, en la Carta de Derechos Fundamentales de la Unión Europea, su art. 8 reconoce el derecho de protección de datos de carácter personal que le conciernan, los que “se tratarán de modo leal, para fines determinados y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley”. Añade la norma que “toda persona tendrá derecho a acceder a los datos recogidos que la conciernan y a su rectificación”, cerrándose el artículo con la mención correspondiente a que “el respeto de estas normas quedará sujeto al control de una autoridad independiente”.

⁹ Naturalmente, la normativa del Consejo de Europa no se agota en el Convenio, pues pueden computarse además, por ejemplo: la Resolución (73) 22 sobre la protección de la intimidad individual frente a los bancos de datos electrónicos en el sector privado, de 26 de setiembre de 1973; la Resolución (87) 15 sobre la utilización de datos personales por la policía, de 17 de setiembre de 1987.

¹⁰ Otras fuentes dignas de mención en el marco comunitario de Europa, v.gr., son: la Resolución del Parlamento Europeo sobre la protección de los derechos de la persona frente al avance de los progresos técnicos en el campo de la informática, de 1979; la Recomendación de la Comisión relativa al mencionado Convenio del Consejo de Europa para la protección de las personas con respecto al procesamiento automático de datos personales, de 1981; la Directiva 2002/58/CE (emitida por el Parlamento y el Consejo en fecha 12 de julio de 2002), relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas.

¹¹ Cfr. PADILLA, MIGUEL M. “La Directiva 95/46/CE de la Unión Europea”, *La Ley*, Buenos Aires, Argentina, 16 de marzo de 1999, pp. 1/2.

Aun colateralmente, debe indicarse que dicha Carta fue proclamada de modo solemne por el Consejo Europeo de Niza en diciembre de 2000, pasando luego a formar parte –íntegramente– del texto de la Constitución Europea (ver Parte II de ésta), aprobada en junio de 2004 y cuyo proceso de ratificación por los Estados Miembros de la Unión Europea se encuentra en curso, aunque –todo debe decirse– el mismo ha recibido en 2005 dos reveses muy importantes –los rechazos de la ciudadanía de Francia y Holanda–, lo que viene a trabar la perspectiva de implementación del mencionado plexo constitucional, al menos en un futuro inmediato.

D. En el contexto de la Organización de los Estados Americanos (OEA), un buen paso adelante significaría la aprobación de una Convención Americana para la Autodeterminación Informativa. Actualmente, sólo existe en etapa embrionaria un borrador o anteproyecto de la misma, en cuyo art. 12, y bajo el epígrafe de “Garantías judiciales”, se prevé el derecho de toda persona a un “recurso” sencillo y rápido o a cualquier otro recurso efectivo ante los jueces o tribunales competentes, que la ampare contra actos que violen sus derechos fundamentales reconocidos por la Convención, la Constitución de los Estados Partes o la ley (art. 12.1). Para tal fin consagra el derecho de toda persona a controlar sus datos personales existentes en ficheros públicos o particulares, señalando que la garantía y el procedimiento judiciales para ejercer tal control es el ‘hábeas data’ (art. 12.2). Además, y si bien refiere al derecho interno de los Estados la regulación de la naturaleza constitucional o común de tal recurso, indica que en todo caso éste debe ser su medio de amparar en forma expedita, rápida y eficaz los derechos de la persona ante los excesos informáticos automatizados o manuales (art. 12.3).

Básicamente el objeto de la protección del anteproyecto de Convención consiste en garantizar, en el territorio de cada Estado Parte, a cualquier persona física o jurídica sean cuales fueren su nacionalidad, residencia o domicilio, el respeto de sus derechos fundamentales, concretamente, su derecho a la autodeterminación informativa con relación a su vida privada y demás derechos de la personalidad, además de la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los datos correspondientes a su persona o bienes (art. 1).

2. En los contextos jurídicos nacionales

A. Europa

Fue Portugal el primer país europeo que reconoció constitucionalmente (en 1976) la necesidad de proteger a las personas frente a los riesgos informáticos. No obstante ello, hubo de transcurrir un período de quince años, para que aquellas disposiciones fueran desarrolladas legislativamente. En efecto, en abril de 1991 se dictó la Ley N° 10 de Protección de datos personales frente a la informática. Tal normativa amplía los parámetros tuitivos de la Constitución; establece que el uso de la informática debe procurarse de forma transparente y con estricto respeto por la reserva de la vida privada y familiar y de los derechos, libertades y garantías fundamentales del ciudadano; prevé la creación de la autoridad de aplicación (Comisión Nacional de Protección de Datos Personales Informatizados); determina que ninguna decisión judicial, administrativa o disciplinaria puede tomarse sobre la exclusiva base del perfil de personalidad del titular del registro del banco de datos; y, en síntesis, reproduce los principios consagrados por el mencionado ‘Convenio

para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal' del Consejo de Europa.

En España, la Constitución de 1978 estableció en los arts. 18.4 y 105, ap. 'b', el diseño del perímetro protectivo genérico de la cuestión, defiriendo en una ley orgánica su tratamiento pomenorizado. El art. 18.4 reza: "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos". Por su parte, el 105, ap. 'b', dispone que la ley regulará: "(b) El acceso de los ciudadanos a los archivos y registros administrativos, salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas". Para dar cumplimiento a la preceptiva constitucional, se dictó el 29 de octubre de 1992, la Ley Orgánica 5 de regulación del tratamiento automatizado de los datos de carácter personal – LORTAD– (BOE N° 262, de 31 de octubre de 1992), abrogada por la Ley Orgánica N° 15/1999, de 13 de diciembre (BOE N° 298, de 14 de diciembre de 1999), que entró en vigor el 14 de enero de 2000, de acuerdo con su disposición final tercera.

En Suecia, la *Datalag*, de 11 de mayo de 1973, además de haber sido el primer antecedente legislativo nacional¹² en Europa, ha ejercido una importante influencia en el contexto de tal continente¹³. Cabe recordar que fue objeto de una modificación por Ley de 1 de julio de 1982 (sobre recolección de datos), además de que la adaptación normativa sueca a la Directiva 95/46/CE se concretó por una ley sancionada el 16 de abril de 1998.

En Francia, debe contabilizarse la Ley N° 78-17 de 6 de enero de 1978, denominada "Ley de Informática, Ficheros y Libertades". Es importante destacar que el 29 de abril de 2004, la Asamblea Nacional adoptó en segunda lectura ciertas modificaciones a dicha ley, cuyas reformas más significativas se centran en el tratamiento de las infracciones, las correspondientes a la protección de datos, la biometría, los servicios secretos y las sanciones pronunciadas por la Comisión Nacional de Informática y Libertades, autoridad de aplicación de la ley.

Para finalizar esta reseña meramente enunciativa, vemos que en Italia oportunamente se dictó la Ley N° 121 de 1 de abril de 1981, además de la posterior normativa legal en vigencia desde el 8 de mayo de 1997 para adecuar sus previsiones a la Directiva 95/46/CE. Por último, actualmente existe el denominado 'Código en materia de protección de los datos personales', según el Decreto legislativo de 30 de junio de 2003, N° 196, con vigor a partir de 27 de febrero de 2004, consolidado con la Ley de 26 de febrero de 2004.

¹² Pues la Ley del *Land de Hesse*, si bien anterior, correspondía a uno de los Estados de la República Federal alemana.

¹³ Así, se ha mencionado que a semejanza suya fueron adoptadas las leyes de protección de datos de Francia, Dinamarca, Noruega y Austria (todas de 1978), Luxemburgo (1979), Israel e Islandia (1981), Reino Unido (1984), la Isla de Man y Guernsey (1986) y en Jersey (1987) cfr. DRESNER, STEWART H. "Panorama de la legislación europea sobre protección de datos personales", trad. de SANTIAGO RIPOLL CARULLA, en *Informática y Derecho*, N° 6/7, UNED - Centro Regional de Extremadura, Mérida, España, 1994, p. 391.

B. América

a. En Estados Unidos de Norteamérica (EE.UU.) y Canadá

Como antecedentes relevantes en EE.UU., podemos ubicar la '*Privacy Act*' y la '*Freedom of Information Act*' (ambas de 1974), para proteger y operativizar el derecho a la privacidad y, paralelamente, impedir la manipulación abusiva de las informaciones.

Asimismo, la '*Freedom of Information Act*', de 1986, que también contiene prescripciones relativas a la revelación de informaciones y a la regulación del derecho de acceso, rectificación o complementación de los registros informáticos.¹⁴

Por su parte, y con la brevedad propia de esta acotada reseña, en Canadá corresponde mencionar la Ley General de Protección de Datos, de 2000, con vigencia desde el 1 de enero de 2001.

b. En el Derecho iberoamericano

Sin perjuicio de nuestra percepción sobre el hábeas data como medio de tutela del derecho a la protección los datos personales por medio de la salvaguarda del derecho de autodeterminación informativa, valga advertir —con EGUIGUREN— que en el ámbito iberoamericano se aprecia una significativa confusión conceptual sobre la naturaleza de la institución del hábeas data (se utilice o no literalmente esa denominación), pues mientras en algunas Constituciones se la regula como una suerte de derecho autónomo (*aspecto sustantivo*) consistente en la denominada “autodeterminación informativa” o la protección frente a los posibles excesos del poder informático en bancos de datos, archivos o registros; en otros casos, se lo define como una garantía o proceso constitucional especial (*aspecto instrumental*) destinado a la protección y defensa de los derechos específicos que en las respectivas normas se señalan¹⁵.

Para desarrollar la reseña propuesta, y luego de desplegado el abanico de soluciones constitucionales existentes, perfilaremos brevemente el movimiento subconstitucional desenvuelto en varios países iberoamericanos en relación con cuestiones referidas directa o indirectamente a la protección de datos personales.

c. En el sentido expuesto, y recorriendo el derecho comparado iberoamericano en punto al particular, vemos que en las Constituciones de Brasil (art. 5.LXXII), Paraguay (art. 135), Perú (art. 200, inc. 3°), Argentina (art. 43, párrafo 3°) y Boli-

¹⁴ Dichos precedentes se mencionan sólo enunciativamente, pues existe una serie de dispositivos normativos sobre el particular, v.gr.: 'Fair Credit Reporting Act', de 1970; 'The Family Education Rights Act', de 1974; 'The Electronic Fund Transfer Act', de 1978; 'The Privacy Protection Act', de 1980 (*vid.* sobre el punto, LUCAS MURILLO DE LA CUEVA, PABLO, cit. *El derecho a la autodeterminación informativa*, pp. 125 y ss.).

¹⁵ EGUIGUREN PRAELI, FRANCISCO J. “Poder Judicial, Tribunal Constitucional y Hábeas Data en el constitucionalismo peruano”, *Cuadernos Constitucionales México-Centroamérica*, N° 35, Centro de Estudios Constitucionales México-Centroamérica, Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México, Corte de Constitucionalidad de Guatemala, México, D.F., 1999, pp. 56/57.

via (art. 23), se focaliza fundamentalmente la acción, garantía, recurso o proceso constitucional (esto es, remarcando el aspecto instrumental)¹⁶. Veamos:

- La Constitución de Brasil —de 1988— fue la primera en incluir en su texto al hábeas data. De hecho, algunos autores brasileños arrojan a dicho país la originalidad en cuanto a la denominación del instituto, sosteniendo que el hábeas data es un *writ* constitucional autóctono. Así, se ha dicho que: “El hábeas data es creación indígena, propiamente nuestra. No tiene un similar específico en el derecho comparado, donde se pueden vislumbrar remedios genéricos que tutelan esa cuestión, mas nunca un remedio determinado, relacionado directamente con la problemática del banco de datos frente al ciudadano”¹⁷. Justo es reconocer, entonces, que la Constitución de Brasil fue la primera que, receptando el instituto, utilizó la terminología de hábeas data, siguiendo los efluvios anticipatorios marcados por la Ley N° 824, de 28 de diciembre de 1984, del Estado de Río de Janeiro.

El plexo constitucional federal preceptúa (en su art. 5.LXXII) que el hábeas data se concede: “a) para asegurar el conocimiento de informaciones relativas a la persona del solicitante, que consten en registros o bancos de datos de entidades gubernamentales o de carácter público”; y “b) para la rectificación de datos, cuando no se prefiera hacerlo por proceso secreto, judicial o administrativo”.

DA SILVA afirma que el hábeas data es un remedio constitucional, un medio dirigido a provocar la actividad jurisdiccional y que, por ese motivo, tiene naturaleza de *acción* (acción constitucional); aunque añade que, paralelamente, contiene un derecho que, en vez de ser reconocido en forma independiente, se encuentra contenido en la garantía que lo ampara¹⁸.

También se ha señalado que Brasil lo reguló como un amparo específico, encaminado a que las personas conozcan las informaciones que les atañen, que se encuentren contenidas en bancos de datos de entidades gubernamentales o públicas. Sintéticamente, tal remedio jurídico-procesal se destina a garantizar al solicitante el ejercicio de su pretensión, bajo tres aspectos: derecho de acceso a los registros; derecho de rectificación; y derecho de complementación de los registros¹⁹.

De una exégesis primaria de la norma constitucional, emerge la limitación en cuanto a la legitimación pasiva, que queda circunscripta a los registros o bancos de datos de carácter gubernamental²⁰ o público, entendiéndose por ‘público’ el que de

¹⁶ Mientras en Brasil, Perú, Paraguay y Bolivia se ha empleado en los respectivos textos constitucionales la expresión ‘hábeas data’, siendo el primero de los países nombrados pionero en tal sentido; en Argentina, por su parte, y si bien no se ha literalizado en la Constitución expresamente tal denominación, existe absoluto consenso tanto en la doctrina como en la jurisprudencia en cuanto a la plasmación de la figura en el artículo constitucional 43, párr. 3°. Además, la Ley N° 25.326 dictada en el ámbito argentino para desarrollar la aludida norma constitucional, ha programado expresamente a partir de su art. 33 la denominada “acción de protección de los datos personales o de *hábeas data*” —énfasis propio—.

¹⁷ ACKEL FILHO, DIOMAR, *Writs constitucionais: habeas corpus, mandado de segurança, mandado de injunção, hábeas data*; Editora Saraiva, São Paulo, Brasil, 1988, p. 115.

¹⁸ DA SILVA, JOSÉ AFONSO, *Curso de Direito Constitucional Positivo*, 8ª ed., Malheiros Editores, São Paulo, Brasil, 1992, pp. 386 y ss.

¹⁹ Cfr. PARANHOS SAMPAIO, LUIZ AUGUSTO, *Comentários à nova Constituição Brasileira*, T° I, Preâmbulo e Arts. 1° ao 17, Edit. Atlas, São Paulo, Brasil, 1989, p. 178.

²⁰ Entidades gubernamentales son todos los organismos públicos o sujetos al control público; órganos de la administración directa del Poder Ejecutivo, entidades autárquicas, empresas públicas, sociedades de economía mixta; y, según ACKEL FILHO (a quien seguimos en la pre-

modo habitual brinde información –publicidad– a terceros; de ello se deduce que la previsión excluye a los registros o bancos de datos estrictamente privados²¹. Del inc. b) de la norma transcripta, se extrae por exclusión la forma de operativizar procesalmente el hábeas data correctivo o rectificatorio, que será utilizado cuando el interesado no prefiera hacerlo por proceso secreto, judicial o administrativo.

Por otra parte, es importante recalcar que el primer inciso del tramo del artículo reproducido *supra*, cuando reza que el hábeas data se concede “para asegurar el conocimiento de informaciones relativas a la persona del solicitante” énfasis propio, patentiza una restricción en torno de la legitimación activa, ya que –al parecer– el único sujeto habilitado para conocer una determinada información es el propio interesado, debiendo tratarse de sus datos personales. Al decir de OTHON SIDOU, tal derecho personalísimo no debe confundirse con el derecho a la información en general que, establecido en el art. 5.XIV, se concede a todos, salvaguardando el secreto de las fuentes cuando sea necesario para el ejercicio profesional²².

En materia de competencia, cabe recordar que ha sido atribuida en forma originaria al Supremo Tribunal Federal cuando el hábeas data se dirige contra actos del Presidente de la República, de las Mesas de la Cámara de los Diputados y del Senado Federal, del Tribunal de Cuentas de la Unión, del Procurador General de la República y del propio Supremo Tribunal Federal; ello, de conformidad con el artículo constitucional 102.I.‘d’. Ya por vía de recurso ordinario, el aludido Supremo Tribunal entiende en las acciones de hábeas data denegadas por los Tribunales Superiores que actuaron en instancia única (cfr. art. 102.II.‘a’ *ibid.*). Por último, OTHON SIDOU advierte que viene deferida al Supremo Tribunal de Justicia el conocimiento, en recurso especial, de los hábeas data respecto de los que los Tribunales Regionales Federales o los Tribunales de los Estados, del Distrito Federal y Territorios hayan dictado sentencia en única o última instancia (art. 105.III, *ibid.*)²³.

Se ha sostenido que la estructura constitucional del hábeas data abarca elementos de los siguientes órdenes: *subjetivo* (*legitimatío ad causam*), *objetivo* (identidad y naturaleza del pedido), *formal* (aspectos concernientes a la competencia jurisdiccional y a la gratuidad de la acción) y *circunstancial* (el problema de la limitación del derecho durante la vigencia del estado de sitio)²⁴; además, y con razón, se ha postulado que la norma en la que se lo vehicula, en tanto contiene los elementos necesarios para su plena actuación, prescinde de la *interpositio legislatoris* (aunque, como veremos, ya se dictó la normativa infraconstitucional), surgiendo –además– la inmediata aplicabilidad de la figura a partir de que el precepto que la contiene identifica los sujetos de la relación procesal, el objeto posible de la postulación judicial y, además, los órganos investidos de competencia jurisdiccio-

cedente apreciación), quedarían incluidos como potenciales legitimados pasivos, los Poderes Legislativo y Judicial (*vid.* ACKEL FILHO, DIOMAR, *op. cit.*, p. 123).

²¹ Se ha apuntado que queda involucrado el banco de datos que, aun cuando administrado por institución privada, ejerza función social de relevancia pública (OTHON SIDOU, J. M., “Las nuevas figuras del derecho procesal constitucional brasileño: mandamiento de ejecución y «hábeas data»”, *La Ley*, T° 1992-E, Buenos Aires, Argentina, p. 1016).

²² *Ídem.*

²³ *Ibid.*, p. 1019.

²⁴ Cfr. las conclusiones de la Opinión N° SR-71 (de 6 de octubre de 1988) de la ‘Consultoría Jurídica de la República’ emitida en el Proceso N° 00400.000014/88-17, en el que figura como parte interesada el Ministro de Estado Jefe del Servicio Nacional de Informaciones –SNI– (apartado ‘j’ de tal dictamen).

nal, concluyéndose en que una eventual dificultad en la aplicación de la regla en cuestión —especialmente en lo que concierne a los aspectos rituales del proceso y de la sentencia—, quedaría superada con el simple empleo de la *analogia legis*, haciendo extensivo al hábeas data, en lo pertinente, la regulación normativa propia de la acción de amparo²⁵.

Para finalizar la referencia al derecho brasileño, cabe mencionar que por medio de la Ley N° 9.507 (de 12 de noviembre de 1997), se ha regulado el derecho de acceso a las informaciones y disciplinado el rito procesal del hábeas data²⁶. En el art. 7 de tal normativa, y además de reiterar los dos objetivos descriptos en el art. 5.LXXII de la Constitución, se ha añadido una tercera finalidad —según DE MORAES—, cual es la de conceder el hábeas data para la anotación en los asientos del interesado de contestación o explicación sobre dato verdadero, mas justificable, y que esté en pendencia judicial o amigable, vislumbrándose con ello la idea de evitar o remediar posibles humillaciones que pueda sufrir el individuo en virtud de datos constantes que, a pesar de ser verdaderos, serían insuficientes para un correcto y amplio análisis, posibilitando una interpretación dudosa o errónea, si no hubiese la oportunidad de mayores esclarecimientos²⁷.

- En el caso de Paraguay, el art. 135 de su Constitución —de 1992— consagra expresamente la garantía de hábeas data (en la Parte I, Título II, Capítulo XII²⁸), diciendo: “ Toda persona podrá acceder a la información y a los datos que sobre sí misma, o sobre sus bienes, obren en registros oficiales o privados de carácter público, así como conocer el uso que se haga de los mismos y de su finalidad. Podrá solicitar ante el magistrado competente la actualización, la rectificación o la destrucción de aquéllos, si fuesen erróneos o afectaran ilegítimamente sus derechos”.

Por tanto, concede el derecho de acceso a la información a los efectos de conocer cuál es el uso o la finalidad para los que se acopian los datos personales del interesado, pudiendo éste solicitar la actualización, rectificación e, incluso, la destrucción de los mismos.

Además, se verifica que el plexo normativo no se detiene sólo en la protección atinente a la información acerca de los derechos extrapatrimoniales del individuo, sino que, también, ofrece resguardo a la conectada con sus intereses patrimoniales. Paralelamente, brinda cobertura a los datos contenidos en los registros oficiales y en los privados.

- Por su parte, el texto primigenio de la Norma Básica del Perú de 1993 (art. 200, inc. 3°) incluye dentro de las garantías constitucionales a la acción de hábeas data, que procede contra el hecho u omisión por parte de cualquier autoridad, fun-

²⁵ Punto '1' del dictámen citado en la nota anterior.

²⁶ Cfr. SABATOVSKI, EMILIO, FONTOURA, IARA P. y FOLMANN, MELISSA, organizadores, *Constituição Federal & Convenções Internacionais*, 8ª ed., Juruá Editora, Curitiba, Brasil, 2001, p. 25.

²⁷ DE MORAES, ALEXANDRE, *Direito Constitucional*, 3ª ed., São Paulo, Brasil, pp. 134/145; citado por PUCCINELLI, OSCAR, *El hábeas data en Indoiberoamérica*, Temis, SantaFé de Bogotá, Colombia, 1999, p. 306.

²⁸ La Parte I se titula: ‘De las declaraciones fundamentales, de los derechos, de los deberes y de las garantías’; el Título II lleva por nombre: ‘De los derechos, de los deberes y de las garantías’; y el Capítulo XII se denomina: ‘De las garantías constitucionales’.

cionario o persona, que vulnere o amenace los derechos consagrados en el art. 2, incs. 5°, 6° y 7°.²⁹

Obviamente, existe una protección más densa pues potencia la acción de hábeas data al declararla articulable contra *cualquier autoridad, funcionario o persona*. Es decir, que no limita la posibilidad de incoar esta “acción de garantía” contra archivos o bancos de datos públicos, sino que también envuelve a los privados. Además, el hábeas data es procedente contra *todo hecho u omisión*.

El último tramo de la norma establecía (ya veremos por qué utilizamos el pretérito) como hipótesis que esa acción u omisión *vulnere o amenace los derechos consagrados en el art. 2 incs. 5, 6 y 7*. Ilustrativamente, recordamos que el inc. 5° establece el derecho a obtener información –en el plazo legal– de cualquier entidad pública, con excepción de las informaciones que afectan la intimidad personal y las expresamente excluidas por ley o por razones de seguridad nacional. El inc. 6° fija el derecho a que los servicios informáticos –computarizados o no, públicos o privados–, no suministren informaciones que afecten la intimidad personal y familiar. Por último, el inc. 7° brinda protección jurídica al derecho al honor y a la buena reputación, a la intimidad personal y familiar, a la voz e imagen propias y al derecho de respuesta.

Huelga poner de resalto que se había hipertrofiado al hábeas data, incluyendo en su seno al derecho de réplica, rectificación o respuesta, circunstancia que fue puesta de manifiesto –según enseña GARCÍA BELAUNDE– a partir de mediados de agosto de 1993 (es decir, muy poco antes de la sanción de la nueva Constitución) por la oposición política, indicándose que el clima podía inclinar la balanza en el sentido de que el hábeas data fuese usado con motivos políticos y para censurar la prensa³⁰.

Tal exceso normativo impuso posteriormente la necesidad de arrancar este derecho de las entrañas del hábeas data, a través de una enmienda constitucional que se concretó en la Ley N° 26.470, publicada en el Diario Oficial “El Peruano” el 12 de junio de 1995, urgida por los reclamos de los medios de comunicación y del Colegio de Periodistas del Perú y rematada por una acción de hábeas data incoada en sede penal por el abogado Vladimir Paz de la Barra, pretensión con la que –conforme da cuenta GARCÍA BELAUNDE– el actor intentó emplear el instituto en forma exagerada, lo que habría desatado una tormenta política que desembocó en la mencionada reforma que llevó sensatez³¹. El sendero procedimental discurrido por la citada acción de Paz de la Barra concluyó con la sentencia de la Corte Suprema de Justicia –Sala Constitucional–, emitida el 28 de marzo de 1994, por la que –sin entrar en el fondo de la cuestión³²– ordenó que la demanda fuera remitida al Juez Especializado en lo Civil de turno.

²⁹ Para profundizar respecto del hábeas data peruano remitimos a ORTECHO VILLENA, VÍCTOR JULIO, *Jurisdicción y procesos constitucionales*, 2ª ed., Edit. Rhodas, Lima, Perú, 1996.

³⁰ GARCÍA BELAUNDE, DOMINGO, *Derecho Procesal Constitucional*, Universidad César Vallejo e Instituto Iberoamericano de Derecho Constitucional (Sección Peruana), Edit. Marsol, Trujillo, Perú, 1998, p. 84.

³¹ *Ibíd.*, pp. 84/85.

³² El accionante exponía como sustento de su acción que en un programa televisivo se había difundido un reportaje según el cual se le atribuía el haber asesorado a un ciudadano en la compra de los denominados “Bonos Alemanes” en perjuicio de los ahorristas de CLAE, además de haberse expresado que los asesores que habían participado en dicha operación eran personajes de dudosa reputación. Por tal razón, solicitaba se ordenara la rectificación de la in-

Al solo efecto ilustrativo, debe recordarse que la previsión constitucional peruana fue posteriormente complementada por la Ley N° 26.301 (dictada el 18 de abril de 1994 por el Congreso Constituyente Democrático y mandada a publicar en mayo de ese año), regulando algunos aspectos de la tramitación procesal del hábeas data y de la acción de cumplimiento. Tal norma fue modificada, derogándose su art. 5, inc. 'b' (específicamente relacionado con la vía previa en la acción de cumplimiento), por medio de la Ley N° 26.545, de 10 de noviembre de 1995.

Finalmente, nos cumple indicar que –en definitiva– aquella Ley N° 26.301 ha quedado actualmente abrogada por la Ley N° 28.237, que aprueba el Código Procesal Constitucional, en vigor desde el 1 de diciembre de 2004 (tema sobre el que volveremos).

- Por su parte, la reforma constitucional argentina que entrara en vigor en agosto de 1994, y dentro de un cúmulo de profundas innovaciones, diseñó normativamente al hábeas data (aunque sin verbalizar dicha expresión), estableciendo en el párrafo 3° del art. 43, que: “Toda persona podrá interponer *esta acción*³³ para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos. No podrá afectarse el secreto de las fuentes de información periodística” –destacado propio–.

No es éste el lugar apropiado para extenderse en consideraciones respecto de la interpretación de la norma constitucional transcrita, aunque sólo mencionaremos que, en cuanto a su configuración normativa en Argentina, el hábeas data posee particularidades propias y específicas que lo separan –y hasta autonomizan– de la acción de amparo. En cualquier caso, negamos que pueda ser encapsulado *simbiotizándolo* a este último³⁴.

- En dirección convergente, es del caso resaltar que, en el supuesto de Bolivia, la Ley de Necesidad de Reformas N° 2.410, publicada el 2 de agosto de 2002, proyectaba incluir tal figura en la Constitución Política, situación que mantuvo y concretó la Ley N° 2.631 de Reforma de la Constitución, de fecha 20 de febrero de 2004, plasmándola en el artículo 23 constitucional, que prefigura al hábeas data como un “recurso” articulable ante la Corte Superior del Distrito o ante cualquier

formación mencionada y la apertura de la instrucción correspondiente; exigía, además, que los periodistas involucrados se abstuvieran en el futuro de relacionarlo con la operación citada, de vincularlo con la CLAE y de referirse a él como personaje de “dudosa reputación”. La juez penal interviniente declaró inadmisibles la acción intentada a través de la sentencia de 7 de febrero de 1994, que fuera confirmada por mayoría en la alzada (en fecha 28 de febrero de idéntico año) y que, elevada a la Corte Suprema, recibiera la respuesta jurisdiccional de que se da cuenta en el texto, es decir, que tal órgano aludió sólo a la competencia (civil) y a que el proceso debía tramitarse de acuerdo con las reglas del procedimiento de amparo, mas omitió expedirse en cuanto a la sustancia del reclamo (El texto de tales fallos han sido consultados en GARCÍA BELAUNDE, DOMINGO, cit., pp. 85/99).

³³ Debe aclararse que, cuando el tramo transcrito dice “*esta acción*”, teóricamente alude a la de amparo, ya que los dos párrafos iniciales del artículo 43 constitucional se refieren a ella. Sin embargo, y como aclaramos escuetamente en el texto, creemos que el hábeas data presenta peculiaridades fisonómicas que lo singularizan diferenciándolo del amparo.

³⁴ Al respecto, reenviamos a BAZÁN, VÍCTOR, “El hábeas data y sus peculiaridades frente al amparo”, *Revista de Derecho Procesal Amparo. Hábeas data. Hábeas corpus – I*, N° 4, Rubinzal-Culzoni Edit., Santa Fe, Argentina, 2000, pp. 215/268.

Juez de Partido a elección suya, órgano que si lo declara procedente, ordenará la revelación, eliminación o rectificación de los datos personales cuyo registro fue impugnado³⁵.

Por su parte, 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.

Más allá del breve adelanto descriptivo precedente, para un mejor entendimiento del precepto que institucionaliza el ‘recurso de hábeas data’, a continuación pasamos a transcribirlo:

“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 Hábeas 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 Hábeas Data no procederá para levantar el secreto en materia de prensa.

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

c. Distinguiéndose –desde los aspectos literal y de técnica de configuración normativa– del conjunto de previsiones constitucionales nacionales analizado *supra*, se aprecia que en las Leyes Fundamentales de Guatemala (art. 31), Colombia (art. 15), Nicaragua (art. 26), Ecuador (art. 94) y Venezuela (art. 28), pareciera ponerse mayor énfasis en el *derecho* a la protección de los datos personales, o sea, en la faceta *sustancial*.

Dicho lo anterior, pasaremos sin más preludios a efectuar una breve reseña de cada una de las cláusulas sobre el particular:

- La Constitución guatemalteca –de 1985–, en su art. 31, y bajo el epígrafe de ‘Acceso a archivos y registros estatales’, establece: “Toda persona tiene el *derecho* de conocer lo que de ella conste en archivos, fichas o cualquier otra forma de registros estatales, y la finalidad a que se dedica esta información, así como a corrección, rectificación y actualización. Quedan prohibidos los registros y archivos de filiación política, excepto los propios de las autoridades electorales y de los partidos políticos” –destacado agregado–.

- La Constitución colombiana –de 1991– en su art. 15, 1º párrafo, reza: “Todas las personas tienen *derecho* a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas” –énfasis añadido–.

³⁵ Para ampliar, véase BAZÁN, VÍCTOR, “El hábeas data en la reforma constitucional boliviana”, en AA.VV., *Análisis de la reforma a la Constitución Boliviana*, Academia Boliviana de Estudios Constitucionales, Edit. El País, Santa Cruz de la Sierra, Bolivia, 2002, pp. 59/107.

do-. El 2° párrafo de tal norma dispone: “En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución” –regresaremos sobre el particular–.

El hábeas data queda incluido en el Capítulo I (“De los Derechos Fundamentales”) del Título II (“De los Derechos, las Garantías y los Deberes”) de la Constitución y, al parecer, se lo diseñó en principio para ser canalizado a través de la acción de tutela, aunque en rigor –según CIFUENTES MUÑOZ– el hábeas data corresponde a un específico proceso constitucional, añadiendo el citado autor que si bien la Corte Constitucional se ha limitado a conferir a la ubicación de los derechos bajo los mencionados capítulo y epígrafe, un valor meramente ilustrativo o indicativo de la naturaleza de un determinado derecho –no enteramente conclusivo–, no se ha puesto jamás en duda que el hábeas data ostente la condición de derecho fundamental³⁶.

- A su turno, el art. 26 de la Constitución de Nicaragua –de 1987, texto según la reforma constitucional implementada por la Ley N° 192, de 1995–, reconoce el derecho de toda persona, “a conocer toda información que sobre ella hayan registrado las autoridades estatales, así como el derecho de saber por qué y con qué finalidad tiene esa información” (num. 4°).

- La Constitución ecuatoriana, de acuerdo con la reforma de 1996 y el texto actualizado en 1998, determina en su art. 94 (localizado en la Sección Segunda: “Del hábeas data”, del Capítulo 6: “De las garantías de los derechos”, del Título III: “De los derechos, garantías y deberes”): “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” –subrayado agregado–.

En los restantes párrafos, aquel artículo prevé sucesivamente que se podrá solicitar ante el funcionario respectivo la actualización de los datos o su rectificación, eliminación o anulación, si fueren erróneos o afectaren ilegítimamente sus derechos; añadiendo que, si la falta de atención causare perjuicio, el afectado podrá demandar indemnización; finalmente, el precepto en cuestión dispone que la ley establecerá un procedimiento especial para acceder a los datos personales que consten en los archivos relacionados con la defensa nacional.

Cabe aún formular una aclaración. Pese a que el citado art. 94, al referirse al hábeas data, pone el acento en el *derecho* de 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; la ‘Ley de Control Constitucional’, promulgada el 2 de julio de 1997, estatuye en su art. 34 que las personas naturales o jurídicas, nacionales o extranjeras, que deseen tener acceso a documentos, bancos de datos e informes que sobre sí mismas o sus bienes están en poder de entidades públicas, de personas naturales o jurídicas privadas, así como conocer el uso y finalidad que se les haya dado o se les esté por dar, podrán interponer el recurso de hábeas data para requerir las respuestas y exigir el cumplimiento de las medidas tutelares prescritas en la Ley, por parte de las personas que posean tales datos o informaciones –remarcado nuestro–.

³⁶ CIFUENTES MUÑOZ, EDUARDO, “El Hábeas Data en Colombia”, *Derecho PUC, Revista de la Facultad de Derecho de la Pontificia Universidad Católica del Perú*, N° 51, diciembre de 1997, public. en 1999, Lima, Perú, p. 122.

- La Constitución venezolana (de 1999) determina que “toda persona tiene *de-recho* de acceder a la información y a los datos que sobre sí misma o sobre sus bienes consten en registros oficiales o privados, con las excepciones que establezca la ley, así como de conocer el uso que se haga de los mismos y su finalidad, y a solicitar ante el tribunal competente la actualización, la rectificación o la destrucción de aquéllos, si fuesen erróneos o afectasen ilegítimamente sus derechos. Igualmente podrá acceder a documentos de cualquier naturaleza que contengan información cuyo conocimiento sea de interés para comunidades o grupos de personas. Queda a salvo el secreto de las fuentes de información periodística y de otras profesiones que determine la ley” –el destacado nos pertenece– (art. 28)³⁷.

HENRÍQUEZ MAIONICA ha sostenido que, de la apreciación del texto de la norma transcripta, surge que toda persona tiene una serie de derechos informáticos, pero como los derechos no se tutelan solos ni son protegidos por otros derechos, su tutela se inserta en las garantías y es, o al menos debe ser, materializada por los jueces, de lo que concluye que la renuncia enunciativa de la garantía de hábeas data no es casualidad sino consecuencia de una fallida técnica legislativa, no por la técnica en sí, sino por el enfoque errático –excesivo literalmente– de los antecedentes normativos del artículo 28 constitucional³⁸.

Por lo demás, a juicio del citado autor, concebir el hábeas data como una categoría de amparo evoca un desconocimiento de la autonomía que, como garantía, el primero de los nombrados tiene³⁹.

Como dato adicional puede puntualizarse que el art. 281, inc. 3º, de la Constitución acuerda legitimación a la Defensoría del Pueblo para interponer –entre otras⁴⁰– la acción de hábeas data. Asimismo, es útil recordar que el art. 60, *ibídem*, expresa en su único aparte que “la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y ciudadanas y el pleno ejercicio de sus derechos”⁴¹.

³⁷ Para interiorizarse acerca de algunos perfiles del hábeas data en la percepción de la Sala Constitucional del Tribunal Supremo de Justicia de Venezuela, pueden verse las sentencias de 23 de agosto de 2000, *in re* “Veedores de la Universidad Católica «Andrés Bello»” Expte. N° 00-2378, Sentencia N° 1.050, y de 14 de marzo de 2001, recaída en el caso *Insaca C.A. vs. Ministerio de Sanidad y Asistencia Social*, (Expte. N° 00-1797, Sentencia N° 332).

³⁸ HENRÍQUEZ MAIONICA, GIANCARLO, “El hábeas data y el derecho de la persona con trastornos de identidad de género a obtener documentos relativos a su identidad biológica”, *Revista de Derecho Constitucional*, N° 8, diciembre de 2003, Edit. Sherwood, Caracas, Venezuela, p. 70.

³⁹ Ídem.

⁴⁰ Nos referimos a las acciones de inconstitucionalidad, amparo, hábeas corpus y los demás acciones o recursos necesarios para ejercer las atribuciones acordadas en los numerales 1º y 2º del art. 281 constitucional, cuando ello fuere procedente de conformidad con la ley.

⁴¹ En la citada Sentencia N° 332, de 14 de marzo de 2001, la Sala Constitucional del Tribunal Supremo de Justicia –relacionando los artículos constitucionales 60, *in fine*, y 28– tuvo ocasión de referir que si la primera de las normas nombradas limita (no prohíbe) el uso de la informática como medio moderno para el registro y almacenamiento de información, debe entenderse que la misma protección (limitación) debe existir para la recopilación de datos e información, que no utilice sistemas computarizados o semejantes; de lo que la Sala extrajo que toda recopilación que exceda los límites legales, además de estar sujeta a los correctivos del comentado artículo 28 constitucional, no podrá hacer prueba en juicio, por ilegítima, excepción que sea contra el recopilador (cfr. ap. VII del fallo).

d. De acuerdo con lo anunciado, puede comprobarse que desde el punto de vista infraconstitucional existe también un importante movimiento legislativo para regular distintos aspectos de la cuestión.

Así, puede constatarse en orden alfabético de los países involucrados que:

- En Argentina, la Ley N° 25.326 de Protección de los Datos Personales, sancionada el 4 de octubre de 2000 y publicada el 2 de noviembre de 2000 (fue observada por el Poder Ejecutivo, por medio del Decreto N° 995/2000), siendo a su vez reglamentada por el Decreto N° 1.558, de 29 de noviembre de 2001, publicado el 3 de diciembre de ese año⁴²;

- en Brasil, como se anticipaba, existe la Ley N° 9.507, de 12 de noviembre de 1997, que ha regulado el acceso a las informaciones y los aspectos procesales del *habeas data*;

- en Chile, la ‘Ley sobre Protección de la Vida Privada’, N° 19.628, publicada en la ‘Gaceta Oficial’ N° 36.860, de 30 de diciembre de 1999, y asimismo, el Decreto N° 779, de 24 de agosto de 2000, que ha reglamentado el Registro de Bancos de Datos Personales a cargo de organismos públicos⁴³;

- en Ecuador, la aludida ‘Ley de Control Constitucional’, que regula al *habeas data* en su capítulo segundo (arts. 34/45).

- en México, la Ley para regular las sociedades de información crediticia (de 2001), publicada en el Diario Oficial de la Federación el 15 de enero de 2002; la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (de 2002, con vigencia a partir de 2003); y algunas normativas sectoriales como la Ley Federal de Protección al Consumidor (de 2000) y la Ley Federal de Derecho de Autor (de 1996, en vigor desde 1997);

- en Paraguay, la Ley N° 1.682, que reglamenta la información de carácter privado, sancionada el 28 de diciembre de 2000; además, existe alguna otra regulación al respecto introducida por vía de una innovación al Código Penal (arts. 141 a 148);

- en Perú, el movimiento legislativo ha sido particularmente intenso. Así, pueden mencionarse –sin ánimo de taxatividad–: la Ley N° 27.489, de 27 de junio de 2001, que rige las centrales privadas de información de riesgos y de protección al titular de la información; la citada Ley N° 28.237, publicada el 31 de mayo de 2004 y en vigor desde el 1 de diciembre de 2004, que aprueba el Código Procesal

⁴² Ilustrativamente, valga evocar que la relativamente reciente reforma constitucional de la Provincia argentina de La Rioja (sancionada y promulgada en marzo de 2002) ha incluido un artículo especial referido al *habeas data* (el 28 bis), consagrando que: “Toda persona física o jurídica podrá interponer acción de *habeas data* para garantizar su derecho de autodeterminación informativa, a cuyo fin está facultada para acceder a sus datos personales y los referidos a sus bienes, y al destino de tal información que se encuentren asentados en archivos, registros, bancos de datos u otros medios técnicos, electrónicos y ópticos, de carácter público o privado, de soporte, procesamiento y provisión de la información; y, en caso de falsedad o uso discriminatorio de tales datos, exigir la supresión, rectificación, actualización o el sometimiento a confidencialidad de los mismos. No podrá afectarse el secreto de las fuentes de información periodística” –énfasis agregado–.

La literalización del derecho de autodeterminación informativa como bien jurídico protegible por el *habeas data* nos parece una solución sumamente positiva y digna de seguimiento por otras normativas constitucionales provinciales que en el futuro se reformen.

⁴³ Colateralmente, puede verse también la Ley N° 19.223 que describe algunos tipos penales relativos a la informática.

Victor Bazán

Constitucional y que, entre otros institutos, regula específicamente al hábeas data como *proceso constitucional* (ver arts. 61 a 65, además de las normas pertinentes a tal figura contenidas en los arts. 1 a 24 que componen el Título I del Código, bajo el siguiente rótulo: ‘Disposiciones generales de los procesos de hábeas corpus, amparo, hábeas data y cumplimiento’); la Ley de Firmas y Certificados Digitales (N° 27.269) y modificatoria (N° 27.310); la Ley que incorpora los delitos informáticos al Código Penal (N° 27.309); la Ley que modifica el Código Civil permitiendo la utilización de los medios electrónicos para la comunicación de la manifestación de voluntad y utilización de la firma electrónica (N° 27.291); la Ley de Notificación por Correo Electrónico (N° 27.419); la Ley de Microformas Digitales (Decreto Legislativo N° 681, Ley N° 26.612 y Decreto Legislativo N° 827); y la Ley de Transparencia y Acceso a la Información Pública (N° 27.806); y

- en Uruguay, la Ley N° 17.838, de ‘Protección de datos personales para ser utilizados en informes comerciales y acción de hábeas data’, publicada el 1 de octubre de 2004, que entrara en vigor diez (10) días después de su publicación en el ‘Diario Oficial’⁴⁴.

IV. SOBRE ALGUNOS LINEAMIENTOS BÁSICOS QUE DEBERÍAN SER TENIDOS EN CUENTA POR LAS FUTURAS REGULACIONES QUE EN LA REGIÓN IBEROAMERICANA SE DICTEN EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

En vista de los distintos proyectos que en diversos países de la región existen (y existieron) en materia de protección de datos personales (por ejemplo, en México, Colombia, Costa Rica⁴⁵, Venezuela, etc.) para dar desarrollo a las disposiciones

⁴⁴ Tal solución viene dispensada por el art. 1 del Código Civil uruguayo, según el cual si la norma en cuestión no prevé otra solución, entra en vigor diez (10) días después de ser publicada.

⁴⁵ Ejemplificativamente, e incluso sin ley reglamentaria, la Sala Constitucional de la Corte Suprema de Justicia costarricense se ha referido a diversas facetas del derecho de autodeterminación informativa en las sentencias N°s 1345-98, 1119-00 y 00754-02 (retornaremos sobre el particular).

Más recientemente, y *mutatis mutandi* (pues no se trata de un supuesto de hábeas data *proprio*—siempre que, *in arguendo*, se aceptara tal escisión categorial—), en la sentencia N° 2004-09705, de 31 de agosto de 2004 (Expte. 03-010830-0007-CO), también hizo alusión expresa al aludido derecho (juntamente con el derecho a la intimidad y el instituto del secreto bancario) como límite al acceso a la información referente a las cuentas corrientes del Partido Liberación Nacional, de la sociedad ‘Proyecciones Nuevo Siglo RAMM S.A.’ y de los señores E.B.S. y R.A.M., en ocasión de resolver el recurso de amparo articulado por un particular (Mauricio Herrera Ulloa, en calidad de periodista del diario ‘La Nación’) y una persona jurídica (precisamente el mencionado periódico), contra el banco ‘Banex S.A.’, ante la negativa de éste a entregarles toda la información solicitada en referencia a las aludidas cuentas corrientes.

En definitiva, la Sala acogió parcialmente el recurso, únicamente en cuanto a la solicitud de información acerca de las cuentas corrientes que tuvieran a su nombre en el banco recurrido la sociedad ‘Proyecciones Nuevo Siglo R.A.M.M. S.A.’ y el Sr. E.B.S., rechazando el recurso en lo restante.

A efectos de operativizar el decisorio, ordenó al apoderado de la entidad bancaria que brindara acceso de forma inmediata a un representante del periódico ‘La Nación’ a la información requerida respecto de los movimientos que se efectuaron en las cuentas corrientes abiertas en

constitucionales respectivas o, en ausencia de éstas, para reglamentar la cuestión directamente por vía legal, juzgamos conveniente advertir que para proporcionar una regulación integral y jurídicamente sustentable del instituto del hábeas data y demás asuntos vinculados con éste y una prefiguración del contenido mínimo del derecho de autodeterminación informativa, la normativa que se intente implementar debería tomar en consideración los siguientes presupuestos básicos y orientativos, que se enuncian sin propósito alguno de exhaustividad:

- Que la recolección de datos personales sea efectuada por medios lícitos (licitud de la captación, consentimiento del interesado, autorización legal, etc.).

- Que la información personal recogida sea utilizada para el fin (lícito) con el que se recolectó (especificidad y justificación social de la recolección).

- Que el tratamiento de los datos personales, además de necesario, sea adecuado, esto es, razonable en función del fin perseguido.

- Que se garantice la calidad de la información personal obrante en el fichero, registro, archivo, base o banco de datos (según la terminología legal escogida), o que se somete a tratamiento.

- Que se limite el tratamiento de información personal intrínsecamente sensible que pudiera generar una discriminación ilegítima o arbitraria.

- Que los datos personales sean conservados durante el tiempo verdaderamente necesario para el cumplimiento de la finalidad para la que fueron captados.

- Que se adopten las medidas protectorias necesarias para evitar el acceso no autorizado, la modificación, la revelación o la destrucción (incluso accidental) de los datos personales⁴⁶ (seguridad de la información).

- Que pueda identificarse de modo sencillo al titular del fichero, registro, archivo, base o banco de datos, a fin de poder –potencialmente– asignarle responsabilidad por el incumplimiento de las obligaciones a su cargo, por su accionar lesivo, etc. (asuntos relativos a la autoridad de aplicación y responsabilidad de los titulares de los registros).

- Que se permita al sujeto interesado debidamente legitimado el derecho de acceso a su información personal contenida en el fichero, registro, archivo, base o banco de datos y, ulteriormente, el derecho de intervención sobre dicha información, es decir, por ejemplo, la posibilidad de rectificarla, suprimirla o someterla a confidencialidad.

ese banco por la sociedad anónima condenada. Asimismo, estableció que debía darse acceso a los movimientos de las cuentas a nombre del Sr. E.B.S., durante los años 1999 a 2002.

Finalmente, indicó que tal orden debía ser acatada bajo entera responsabilidad del periódico 'La Nación' y del periodista Mauricio Herrera Ulloa respecto del uso que se hiciera de dicha información, que debía estar limitada a los movimientos relacionados con la pasada campaña electoral, sin que pudiera el periódico recolectar, almacenar o hacer uso de cualquier otra información extraíble de las cuentas a las que accedería.

⁴⁶ Cfr. LOSANO, MARIO; en LOSANO, MARIO, PÉREZ LUÑO, ANTONIO-ENRIQUE y GUERRERO MATEUS, MARÍA FERNANDA, *Libertad informática y leyes de protección de datos personales*, en *Cuadernos y Debates*, N° 21, Centro de Estudios Constitucionales, Madrid, España, 1989, p. 67.

V. ANÁLISIS PARTICULARIZADO DEL DERECHO DE AUTODETERMINACIÓN INFORMATIVA⁴⁷

1. Aproximación conceptual

Es conveniente independizar conceptualmente el derecho de autodeterminación informativa, como bien jurídico protegido por el hábeas data, de derechos personalísimos tales como el de intimidad, al honor o a la imagen, y aun a la identidad, sin desconocer que tienen puntos de confluencia en tanto el de autodeterminación informativa, más allá de su dimensión *sustancial*, ofrece una valiosa vertiente *instrumental* –*inter alia*– de aquel conjunto de derechos.

El derecho de autodeterminación informativa consiste en la posibilidad que tiene el titular de los datos personales de controlar quiénes serán destinatarios de éstos y qué uso les darán, y se ejercita genéricamente a través de los derechos de acceso, rectificación y cancelación. Además, ofrece una textura que resulta acorde con los modernos desafíos informáticos, puesto que, abandonando el concepto de intimidad como libertad negativa, permite avanzar hacia una fase *activa* del proceso de circulación de la información personal brindando protagonismo al interesado al posibilitarle el ejercicio de un adecuado control sobre la misma.

Como se afirmara, el derecho de la autodeterminación informativa es un derecho a saber y también un derecho a la transparencia del procesamiento de datos, el cual a su vez es una parte fundamental del concepto moderno de democracia⁴⁸.

RIANDE JUÁREZ señala que con el establecimiento de dicho derecho se distribuye el ejercicio del control sobre el tratamiento de los datos personales, por una parte, a la sociedad en general, que establece los criterios de acuerdo con los cuales se permite el manejo de tales datos; y, por otra, los individuos deciden si consienten o no que otros manejen sus datos⁴⁹. Además, el Estado deberá vigilar la aplicación de aquellos criterios mediante la entrega en concesión del derecho al procesamiento de datos personales a quienes acepten realizarlo responsabilizándose de vigilar que se respete el derecho de autodeterminación informativa en los términos de la reglamentación prevista, y quienes manejen tales datos tendrán que participar activamente en las tareas necesarias para proteger a éstos.

Asimismo, con acierto se ha precisado que el derecho de autodeterminación informativa no sólo tiene validez para el almacenamiento de los datos, sino también a lo largo de todo el proceso de obtención de la información, de tal manera que la

⁴⁷ Entre otros trabajos de BAZÁN, VÍCTOR, ver por ejemplo sobre el epígrafe consignado en el texto: “Del concepto preinformático de la intimidad al derecho de autodeterminación informativa”, en AA.VV., *El cuarto poder. Expresión, información y comunicación social*, Instituto de Investigaciones Jurídicas y Sociales ‘Ambrosio L. Gioja’, Facultad de Derecho y Ciencias Sociales, Universidad de Buenos Aires, Ediar, Buenos Aires, Argentina, 1999, pp. 49/158; “El hábeas data entre el misonéismo y la desprotección de los derechos fundamentales”, *Voces Jurídicas*, T° 2, Mendoza, Argentina, abril de 1997, pp. 35/60; “Hábeas data y autodeterminación informativa”, *Revista Jurídica del Perú*, Año XLVI, N° 3, julio-septiembre de 1996, Trujillo, Perú, pp. 57/84.

⁴⁸ CHIRINO SÁNCHEZ, ALFREDO, “Algunas reflexiones acerca de la tutela penal de la autodeterminación informativa. El caso del Proyecto de Código Penal costarricense de 1995”, *Nueva Doctrina Penal*, Vol. 1997-A, Editores del Puerto, Buenos Aires, p. 104.

⁴⁹ RIANDE JUÁREZ, NOÉ A. “Privacidad, autodeterminación informativa y la responsabilidad de proteger los bienes de uso común”, *Derecho y nuevas tecnologías*, Año 3, Número Especial 4/5 ‘Derechos personalísimos’, Edit. Ad-Hoc, Buenos Aires, Argentina, 2003, p. 69.

forma de almacenamiento de los datos (manual o electrónica) no tiene un verdadero papel fundamental⁵⁰.

2. Prefiguración jurisprudencial

En una célebre sentencia, de 15 de diciembre de 1983, al tiempo de declarar parcialmente inconstitucional la Ley del Censo de Población de 1982, el Tribunal Constitucional alemán precisó los perfiles del derecho de autodeterminación informativa.

PÉREZ LUÑO expresa que el mérito de dicho fallo reside en haber entendido al derecho a la intimidad como expresión del derecho a la autodeterminación informativa; es decir, como una facultad de la persona de “decidir básicamente por sí misma cuándo y dentro de qué límites procede revelar situaciones referentes a la propia vida”. Por tal razón es que el Tribunal germano concluye que contrariaría a dicho derecho de autodeterminación informativa “un orden social y un orden jurídico que hiciese posible al primero, en el que el ciudadano ya no pudiera saber quién, qué, cuándo y con qué motivo sabe algo sobre él (...) Esto no sólo menoscabaría las oportunidades de desarrollo de la personalidad individual, sino también el bien público, porque la autodeterminación constituye una condición elemental de funcionamiento de toda comunidad fundada en la capacidad de obrar y de cooperación de sus ciudadanos”⁵¹.

Como dato previo a la determinación de los perfiles del derecho de autodeterminación informativa a cargo del *Bundesverfassungsgericht* en la referida sentencia, LUCAS MURILLO DE LA CUEVA ubica el hecho de que a la percepción de la insuficiencia de la noción tradicional de la intimidad ante los riesgos que despuntaban, se le adjuntó la exigencia de incorporarle la *intimidad informativa*, expresión que aparece en los ‘60 en diversos autores americanos (WESTIN, MILLER, ALPA, HIXSON)⁵². Indica a continuación el citado autor español que, a partir de tal distinción, se construyó el sistema británico de protección de datos, ya que durante el extenso período de trabajos preparatorios se confeccionó –*inter alia*– el ‘Informe Younger’, que diferenciaba dos facetas de la intimidad: la intimidad física y la intimidad informativa⁵³.

Si bien existe consenso en resaltar la importancia de la mencionada sentencia del Tribunal Constitucional Federal alemán en la delineación fisonómica del derecho de autodeterminación informativa, DENNINGER plantea algunas reservas al respecto, sosteniendo que ni el objeto ni la terminología del aludido derecho pueden tomarse como una originalidad de aquel Tribunal, ya que –en lo atinente al objeto– se trata del producto de una extensa evolución jurisprudencial encaminada al reconocimiento y a la elaboración del derecho general a la personalidad; y, en lo concerniente a la denominación, en tanto la misma había sido empleada por la doctrina jurídica alemana desde 1971.

⁵⁰ CHIRINO SÁNCHEZ, ALFREDO, *op. cit.*, p. 104.

⁵¹ PÉREZ LUÑO, ANTONIO-ENRIQUE, “La defensa del ciudadano y la protección de datos”, *Jornadas Internacionales sobre Informática y Administración Pública*, Herri-Andulararit, Zaren Euskal Erakundea, Instituto Vasco de Administración Pública, Oñati, Colección Administración y Autonomía, 1986, pp. 58/59.

⁵² LUCAS MURILLO DE LA CUEVA, PABLO, *cit. El derecho a la autodeterminación informativa*, pp. 120/121.

⁵³ *Ibid.*, p. 121.

No obstante las objeciones expuestas en palabras de PÉREZ LUÑO, DENNINGER “reconoce que la sentencia ha supuesto una contribución muy valiosa para la garantía jurisdiccional de la protección de los datos personales, así como para la concreción del derecho a la autodeterminación informativa, entendido como el presupuesto para el funcionamiento de los sistemas informatizados de tratamiento de datos en un Estado de Derecho inspirado en los principios de la libertad y la democracia”⁵⁴.

3. ¿Es suficiente el concepto preinformático de intimidad frente a la necesidad de proteger los datos personales?

Si bien existe una estrecha conexión entre los elementos del tándem informática-intimidad, debe quebrarse ideológicamente su presunta indisolubilidad pues ésta termina por opacar el meollo del problema y conduce a una confusión entre el fenómeno y su premisa, dado que —como afirma JIMÉNEZ ESCOBAR— en diversas oportunidades la agresión a la intimidad constituye un antecedente previo y necesario para la posterior recolección, tratamiento y comunicación ilegítimos de los datos personales⁵⁵, algunos de los cuales aun cuando no siendo *íntimos* pero sí *sensibles*, igualmente reclamarán protección jurídica.

Es que, ante el problema que para el Derecho implicaba encuadrar la irrupción informática en una categoría jurídica, aquél halló en la intimidad la respuesta apropiada, desde que —como se expusiera— “el derecho a la intimidad era una libertad fundamental perfectamente estudiada, nacida como categoría jurídica el siglo pasado se refiere al S. XIX y sin el abo­lengo de otros derechos humanos, pero totalmente definida, acotada, documentada. Acudir a esta categoría evitaba la fatigosa tarea de crear un nuevo derecho (o el tener que prescindir de un determinado derecho) al que designar como objeto de la agresión de la nueva tecnología”⁵⁶.

El derecho de autodeterminación informativa, como bien jurídico tutelado por el hábeas data, tiene por objeto, entonces y como verifica LUCAS MURILLO DE LA CUEVA, “preservar la información individual —íntima y no íntima— frente a su utilización incontrolada, arrancando, precisamente, donde termina el entendimiento convencional del derecho a la vida privada”⁵⁷.

⁵⁴ Vid. PÉREZ LUÑO, ANTONIO-ENRIQUE, *op. cit.* en nota 51, “La defensa del ciudadano...”, p. 61. El autor y el trabajo citados por PÉREZ LUÑO se ajustan al siguiente detalle: DENNINGER, ERHARD, “Das Recht auf informationelle Selbstbestimmung und inhere Sicherheit”, en *Informationsgesellschaft oder Überwachungsstaat. Strategien zur Wahrung der Freiheitsrechte im Computerzeitalter*, Actas del Symposium celebrado en Wiesbaden de 3 a 5 de septiembre de 1984, Hessendienst der Staatskanzlei, Wiesbaden, RFA, 1984, pp. 291 y ss.

⁵⁵ JIMÉNEZ ESCOBAR, R. “Informática y derecho a la intimidad: una concepción que debe arrumbarse”, en *Jornadas Abogacía e Informática*, p. 85; cit. por GONZÁLEZ MURÚA, ANA ROSA, “Comentario a la S.T.C. 254/1993, de 20 de julio. Algunas reflexiones en torno al artículo 18.4 de la Constitución y la protección de los datos personales”, en *Informática y Derecho*, N° 6/7, cit., pp. 242/243.

⁵⁶ JIMÉNEZ ESCOBAR, R. *op. cit.* nota anterior, p. 243.

⁵⁷ LUCAS MURILLO DE LA CUEVA, PABLO, cit. *El derecho a la autodeterminación informativa*, p. 120.

Ilustrativamente, y *mutatis mutandi*, reenviamos al Tribunal Constitucional español que, por ejemplo en la STC 292/2000⁵⁸, de 30 de noviembre, ha mencionado al respecto: “Sin necesidad de exponer con detalle las amplias posibilidades que la informática ofrece tanto para recoger como para comunicar datos personales ni los indudables riesgos que ello puede entrañar, dado que una persona puede ignorar no sólo cuáles son los datos que le conciernen que se hallan recogidos en un fichero sino también si han sido trasladados a otro y con qué finalidad, es suficiente indicar ambos extremos para comprender que el derecho fundamental a la intimidad (art. 18.1 CE⁵⁹) no aporte por sí sólo una protección suficiente frente a esta nueva realidad derivada del progreso tecnológico”. (Fundamento Jurídico —en adelante, también, FJ— 4°).

En dirección convergente, la citada sentencia reza en otro de sus segmentos: “...el objeto de protección del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal. Por consiguiente, también alcanza a aquellos datos personales públicos, que por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos. También por ello, el que los datos sean de carácter personal no significa que sólo tengan protección los relativos a la vida privada o íntima de la persona, sino que los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo” —énfasis propio— (FJ 6°).

4. Acerca de los llamados “datos sensibles”

Otra cuestión de interés que cabe presentar aquí —y que fue anticipada *supra*— es la concerniente a los denominados “datos sensibles”, que —genéricamente— pueden ser conceptuados como los “datos personales que revelan origen racial y étni-

⁵⁸ En tal sentencia abordó el recurso de inconstitucionalidad N° 1463-2000, interpuesto por el Defensor del Pueblo, contra los arts. 21.1 y 24.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

En definitiva, estimó el mencionado recurso de inconstitucionalidad y, en consecuencia, declaró contrario a la Constitución y nulo el inciso “cuando la comunicación hubiere sido prevista por las disposiciones de creación del fichero o por disposición de superior rango que regule su uso o” del apartado 1 del art. 21 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Asimismo, declaró contrarios a la Constitución y nulos los incisos “impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones públicas” y “o administrativas” del apartado 1 del art. 24, y todo su apartado 2, de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

⁵⁹ Norma que determina que “se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen”.

co, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual”⁶⁰.

Acertadamente, se ha postulado que la necesidad de establecer jurídicamente medidas de protección de los datos personales frente a la informatización, se debe no tanto al carácter privado que algunos de ellos puedan tener, sino a las múltiples posibilidades de elaboración e interrelación propias de la tecnología informática, pues como ha sostenido el Tribunal Constitucional Federal alemán en la citada sentencia sobre la Ley del Censo, “un dato carente en sí mismo de interés puede cobrar un nuevo valor de referencia y, en esta medida, ya no existe, bajo las condiciones de la elaboración automática de datos, ninguno ‘sin interés’”⁶¹.

No deja de ser sugerente la percepción de CHIRINO SÁNCHEZ, quien advierte que el riesgo de la construcción de perfiles de personalidad, a través de los cuales es posible catalogar a los ciudadanos y a los grupos sociales, y tomar medidas de prevención social así como otras medidas de control, está en la base misma de la reflexión del Tribunal alemán en el mencionado decisorio, ya que cuando el mismo afirma que no existen ya más datos sin interés, se está refiriendo al hecho de que, para la construcción de perfiles de los ciudadanos, cualquier detalle, característica, circunstancia o evento en su vida, que de cualquier otra manera pasaría desapercibido, es de una importancia decisiva para los fines del control estatal⁶².

Es necesario advertir que existen datos en apariencia inocuos o irrelevantes que, de modo súbito, se convierten en extremadamente sensibles mediante un sencillo cambio del fin que se persiguiera al momento de su recolección.

Lo anterior pone de manifiesto —como expresa OROZCO PARDO⁶³— que un dato es inocuo o sensible, no ya por su contenido, sino por el uso que de él se haga. Por tanto, preliminarmente, sólo indicaremos que el énfasis debe ser puesto en el fin para el que se emplea la información colectada⁶⁴, por lo que las garantías tuitivas del derecho de autodeterminación informativa deberían focalizar la utilización que de la información se haga —dirección hacia la que apuntan ciertas tendencias jurisprudenciales evidenciadas, v.gr., en Alemania e Italia—, y no tanto la calificación apriorística de si un dato es sensible o no lo es⁶⁵.

En función de todo ello, creemos adquirirá relevancia superlativa la tarea judicial para desentrañar si en el caso concreto sobre el que debe el juez fallar, la información personal de que se trate —con prescindencia de si *a priori* es o no sensible—, ha sido sometida a un empleo discriminatorio, perjudicial, descontextualizado, etc.

⁶⁰ Hemos utilizado como marco referencial la definición que al respecto proporciona la Ley argentina N° 25.326 (art. 2).

⁶¹ LUCAS MURILLO DE LA CUEVA, PABLO, *op. cit. El derecho a la autodeterminación informativa*, p. 122.

⁶² CHIRINO SÁNCHEZ, ALFREDO, *op. cit.*, p. 105.

⁶³ OROZCO PARDO, GUILLERMO, “Consideraciones sobre los derechos de acceso y rectificación en el proyecto de Ley Orgánica de Regulación del tratamiento automatizado de los datos de carácter personal”, *Informática y Derecho*, N° 5, UNED - Centro Reg. de Extremadura, Ed. Aranzadi, Mérida, España, 1994, p. 222.

⁶⁴ Ello no implica desdeñar la existencia de datos *intrínsecamente* sensibles, sino de propiciar una visualización *dinámica* de la tutela que la información de carácter personal merece.

⁶⁵ Cftar. PÉREZ LUÑO, ANTONIO-ENRIQUE, ‘III Congreso Iberoamericano de Informática y Derecho’, Coloquios, Mesa N° 2, en *Informática y Derecho*, N° 5, *loc. cit.* en nota 63, p. 364.

5. *El de autodeterminación informativa, ¿es un derecho autónomo?*

Desde nuestra óptica, y en función de lo mencionado precedentemente, todo indica que el de autodeterminación informativa es un derecho autónomo, con una doble dimensión: *sustancial*, como derecho en sí mismo; e *instrumental*, es decir, como soporte para la cobertura tuitiva de otros derechos, por ejemplo, del de intimidad, honor, dignidad –tema sobre el que volveremos–.

Para corroborar tal aserto (carácter autonómico de tal derecho), no deja de ser útil compulsar la creciente tendencia que exhibe la jurisprudencia comparada al respecto.

En ese sentido, y como recuerda CHIRINO SÁNCHEZ, en sentencias posteriores a la relativa a la Ley del Censo de Población, el Tribunal Constitucional alemán se ha referido al derecho en cuestión como el “derecho fundamental a la autodeterminación informativa”, por ejemplo, en el decisorio publicado en *Neue Juristische Wochenschrift*, 1991, p. 2132⁶⁶.

Por su parte, del examen del itinerario jurisprudencial del Tribunal Constitucional español surge que una de las cuestiones que genera el análisis de la STC 254/1993, de 20 de julio, es la relación entre el derecho a la intimidad y el derecho a la autodeterminación informativa. En dicho pronunciamiento se esgrimió por vez primera el citado art. 18.4 de la CE, en el caso de un ciudadano a quien el Gobierno Civil de Guipúzcoa le denegó información acerca de los datos que sobre su persona poseía.

Concretamente, en su FJ 6º, la sentencia dispone: “...nuestra Constitución ha incorporado una nueva garantía constitucional como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona, de forma en último término no muy diferente a como fueron originándose e incorporándose históricamente los distintos derechos fundamentales. En el presente caso estamos ante un instituto que es, en sí mismo, un derecho fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama «la informática»”.

El análisis de la posición del Tribunal Constitucional ha provocado visiones doctrinarias discordantes. Así, mientras algunos afirman contundentemente que la sentencia admite que del artículo 18.4 constitucional se deduce un derecho fundamental autónomo: la libertad informática⁶⁷; otros, arriban a la conclusión contraria⁶⁸.

Desde nuestra perspectiva, de la lectura del mencionado FJ 6º surge que el Tribunal Constitucional se expidió por la existencia de un derecho fundamental autónomo, diverso del contenido en el art. 18.1 C.E, aun cuando no emplee la nomenclatura “derecho a la autodeterminación informativa”.

⁶⁶ Cfr. CHIRINO SÁNCHEZ, ALFREDO, *op. cit.*, p. 107.

⁶⁷ Entre otros, LUCAS MURILLO DE LA CUEVA, PABLO, “La construcción del derecho a la autodeterminación informativa” (www.csi.map.es/csi/tecniomap/tecniomap1998/sp14.htm).

⁶⁸ Por ejemplo, VILLAVERDE MENÉNDEZ, IGNACIO, “Protección de datos personales, derecho a ser informado y autodeterminación informativa del individuo. A propósito de la STC 254/93”, *Revista Española de Derecho Constitucional*, N° 41, mayo-agosto 1994, Centro de Estudios Políticos y Constitucionales, Madrid, España, pp. 187 y ss.

Además, dicho derecho fundamental autónomo a la protección de datos personales ha sido paulatinamente perfilado en pronunciamientos posteriores del Tribunal. En efecto, fue conformándose en la decisión relativa a las normas reguladoras del número de identificación fiscal (STC 143/1994, de 9 de mayo); también, en la que declaró contrario a la libertad sindical (art. 28 CE), en relación con el art. 18.4 CE, el uso por una empresa del dato de la afiliación sindical para detraer haberes de los trabajadores con ocasión de una huelga promovida por determinado sindicato (STC 11/1998⁶⁹, de 13 de enero); o la STC 202/1999, de 8 de noviembre, en la que, con ocasión de la denegación a un trabajador de la cancelación de sus datos médicos en un fichero informatizado de una entidad de crédito sobre bajas por incapacidad temporal, se apreció que el almacenamiento sin cobertura legal en soporte informático de los diagnósticos médicos del trabajador sin mediar su consentimiento expreso, constituía una desproporcionada restricción del derecho fundamental a la protección de datos personales.

En las mencionadas sentencias el Tribunal declaró que el art. 18.4 CE contiene, en los términos de la STC 254/1993, un instituto de garantía de los derechos a la intimidad y al honor y del pleno disfrute de los restantes derechos de los ciudadanos que, además, es en sí mismo "un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama 'la informática'", lo que se ha dado en llamar "libertad informática" (FJ 6º, reiterado luego en las SSTC 143/1994, FJ 7º; 11/1998, FJ 4º; 94/1998, FJ 6º; 202/1999, FJ 2º).

Sea como fuera, en las SSTC 290/2000⁷⁰ (FJ 7º) y 292/2000 (ya aludida) –FJ 5º–, ambas de 30 de noviembre de 2000, ha aclarado debidamente la cuestión, al señalar que el derecho fundamental a la protección de datos personales frente a la informática o, si se quiere, a la "libertad informática" (reenviando a la citada STC 254/1993) garantiza a la persona un poder de control y disposición sobre sus datos personales, pues confiere a su titular un haz de facultades que son elementos esenciales del derecho fundamental a la protección de los datos personales, integrado

⁶⁹ Doctrina que ha sido reiterada en una serie de sentencias del Tribunal expidiéndose sobre idéntica problemática, entre las merece especial atención la STC 94/1998, de 4 de mayo.

⁷⁰ En tal sentencia el Tribunal resolvió los recursos de inconstitucionalidad acumulados N.ºs. 201/93, 219/93, 226/93 y 236/93, interpuestos respectivamente por el Consejo Ejecutivo de la Generalidad de Cataluña, el Defensor del Pueblo, el Parlamento de Cataluña y por don Federico Trillo-Figueroa Conde, Comisionado por 56 Diputados del Grupo Parlamentario Popular, contra los arts. 6.2, 19.1, 20.3, 22.1 y 2.1, 24, 31, 39.1 y 2, 40.1 y 2, y Disposición final tercera de la Ley Orgánica 5/1992, de 29 de octubre, de la LORTAD, que ya había sido derogada por la Ley Orgánica de Protección de Datos de Carácter Personal (LOPD), publicada en el BOE de 14 de diciembre de 1999, en virtud de su Disposición derogatoria única, aunque tal derogación no alcanzaba de inmediato, por lo dispuesto en la Disposición transitoria tercera de la segunda de dichas Leyes, a las normas reglamentarias vigentes dictadas para su desarrollo que allí se citan, en cuanto no se opongan a la nueva Ley, que continuarían en vigor hasta que no se llevase a efecto lo prevenido en la Disposición final primera.

Con el voto particular del Magistrado don Manuel Jiménez de Parga y Cabrera, el Tribunal declaró, en cuanto a los arts. 6.2, 19.1, 20.3, 22.1 y 2.1, 39.1 y 2 y Disposición final tercera de la LORTAD, la pérdida sobrevenida del objeto de los recursos interpuestos por los Diputados del Grupo Parlamentario Popular y por el Defensor del Pueblo. Asimismo, desestimó los recursos interpuestos por el Consejo Ejecutivo de la Generalidad de Cataluña y el Parlamento de Cataluña contra los arts. 24, 31 y 40.1 y 2 de dicha Ley Orgánica.

por los derechos que corresponden al afectado a consentir la recogida y el uso de sus datos personales y a conocer los mismos. Y para hacer efectivo ese contenido, el derecho a ser informado acerca de quién posee sus datos personales y con qué finalidad, así como el derecho a oponerse a esa posesión y uso exigiendo a quien corresponda que ponga fin a la posesión y empleo de tales datos. Añade que, en suma, el derecho fundamental comprende un conjunto de derechos que el ciudadano puede ejercer frente a quienes sean titulares, públicos o privados, de ficheros de datos personales, partiendo del conocimiento de tales ficheros y de su contenido, uso y destino, por el registro de los mismos.

Fuera del contexto español, también ofrece alguna percepción compatible con la autonomía del derecho en cuestión, la jurisprudencia de la Corte Constitucional de Colombia, la que ha variado su percepción al respecto, pues mientras en un primer momento —de acuerdo con lo que asevera CIFUENTES MUÑOZ— no dudó en acomodar conceptualmente al *habeas data* dentro del ámbito del derecho a la intimidad (Sentencia T-414, de 16 de junio de 1992), posteriormente, en la sentencia de unificación jurisprudencial SU-082, de 1 de marzo de 1995, rectificó el anterior criterio y atribuyó al *habeas data* una configuración autónoma y propia, señalando que el núcleo esencial del *habeas data* estriba en la defensa del derecho a la “autodeterminación informática” (*sic*), en cuya virtud la persona a la cual se refieren los datos que reposan en un archivo público o privado está autorizada para permitir su conservación, uso y circulación⁷¹.

Por su parte, y ya respecto de la doctrina judicial de Costa Rica, elaborada por la Sala Constitucional de la Corte Suprema de Justicia, CARVAJAL PÉREZ destaca que se observan por un lado, las sentencias N^{os}. 4154-97, 7175-97, 4347-99 y 5802-99 que reconocieron la existencia de un derecho a la tutela jurisdiccional privilegiada de los datos personales (*habeas data*), desarrollando una serie de principios atinentes al acopio, almacenamiento y empleo de bases de datos, lista que ha sido ampliada y delimitada por diversos fallos posteriores, tales como las sentencias N^{os}. 1345-98, 1119-00 y 00754-02, que reconocen expresamente la existencia de un derecho a la autodeterminación informativa y desarrollan en detalle sus postulados esenciales —remarcado propio—, en particular el principio de calidad de los datos y de adecuación al fin para el cual fueron obtenidos⁷².

Según el autor que citamos, esta trilogía de sentencias demuestra que la Sala Constitucional costarricense decidió entender en forma amplia la relación existente entre el derecho a la intimidad y el principio democrático, observándola como un presupuesto esencial para el ejercicio de otros derechos fundamentales previstos en la Constitución, que definen al ciudadano como una entidad que actúa libre, interactuando con otros y desarrollando su plan de vida libre de intervenciones estatales o privadas, mientras este plan no entre en contradicción con las bases del sistema⁷³.

⁷¹ Cfr. CIFUENTES MUÑOZ, EDUARDO, cit. pp. 122 y 123.

⁷² CARVAJAL PÉREZ, MARVIN, “Tutela constitucional del derecho a la autodeterminación informativa en Costa Rica”, trabajo presentado en el Taller N° 4: ‘Libertad de expresión, vida privada e Internet’, del “VI Congreso Mundial de Derecho Constitucional”, organizado por la Asociación Internacional de Derecho Constitucional, Santiago, Chile, enero de 2003.

⁷³ Ídem.

6. El carácter instrumental del derecho de autodeterminación informativa

Como anunciábamos, más allá de la perspectiva sustancial, no debe soslayarse que el derecho de autodeterminación informativa presenta un carácter *instrumental* para la efectivización de otros derechos.

Tal premisa se hizo patente, por ejemplo y buceando en la jurisprudencia del Tribunal Constitucional español, en la STC 11/1998⁷⁴, en la que el derecho a la autodeterminación informativa se empleó como instrumental al de libertad sindical reconocido por el art. 28.1 de la Constitución de ese Reino⁷⁵.

Como afirma LUCAS MURILLO DE LA CUEVA –comentando tal vertiente del derecho a la autodeterminación informativa–, si la protección de la información personal ante los peligros derivados de su tratamiento automatizado es un bien jurídico valioso por sí mismo, también posee una dimensión instrumental en la medida en que sirve para garantizar otros derechos⁷⁶. Señala, asimismo, que si esta doble cualidad no es ajena a los derechos fundamentales, lejos de devaluarlos, incrementa su relevancia⁷⁷.

7. De la “relatividad” del derecho de autodeterminación informativa. Aproximación jurisprudencial

Para evitar la parcialización del enfoque que intentamos trasuntar, entendemos que el de la autodeterminación informativa es, en tanto derecho, relativo. El límite que se erige frente a su despliegue vivencial viene marcado por el innegable valor que asume la información como bien colectivo en el conjunto social. Asimismo, no debería soslayarse la necesidad de imponer un tratamiento democrático de la información, procurando conglobar los esfuerzos (públicos y privados) para lograr un sano equilibrio axiológico de los bienes en interacción.

En conexión con ello, está claro que la percepción que el Tribunal Constitucional alemán evidenciara en la retrocitada sentencia de 1983 y que trasunta la mencionada relatividad del derecho a la autodeterminación informativa, pone de manifiesto la necesidad de no olvidar la perspectiva social y comunitaria de éste⁷⁸, evitando –de acuerdo con la visión de SIMITIS⁷⁹– que el mismo sea concebido exclusivamente bajo el tamiz individualista y patrimonial.

⁷⁴ Sentencia que, junto a otras (N^{os}. 33, 35 y 94 –todas de 1998–), giraba en torno de la utilización por una empresa de datos personales relativos a la afiliación sindical de sus trabajadores para fines distintos de los que motivaron su recolección.

⁷⁵ Que dispone: “Todos tienen derecho a sindicarse libremente. La ley podrá limitar o exceptuar el ejercicio de este derecho a las Fuerzas o Institutos armados o a los demás Cuerpos sometidos a disciplina militar y regulará las peculiaridades de su ejercicio para los funcionarios públicos. La libertad sindical comprende el derecho a fundar sindicatos y a afiliarse al de su elección, así como el derecho de los sindicatos a formar confederaciones y a fundar organizaciones sindicales internacionales o afiliarse a las mismas. Nadie podrá ser obligado a afiliarse a un sindicato”.

⁷⁶ LUCAS MURILLO DE LA CUEVA, PABLO, cit., La construcción del derecho a la...

⁷⁷ Ídem.

⁷⁸ PÉREZ LUÑO, ANTONIO-ENRIQUE, “Los derechos humanos en la sociedad tecnológica”, en LOSANO, MARIO G., PÉREZ LUÑO, ANTONIO-ENRIQUE y GUERRERO MATEUS, MARÍA FERNANDA, *op. cit.*, p. 156.

⁷⁹ SIMITIS, SPIROS, “Datenschutz. Voraussetzung oder Ende der Kommunikation?”, en *Europäische Rechtsdenken in Gesichte und Gegenwart. Festschrift für Helmut Coing zum 70 Ge-*

HASSEMER señala que el desarrollo del derecho a una protección de datos personales se alimenta, en las sociedades modernas, de dos fuentes: de la tempestuosa marcha triunfal de la tecnología de la información, en conjunto con el escepticismo sobre el Estado y lo que de éste puede esperarse⁸⁰. Añade el catedrático alemán que, en la República Federal de Alemania (RFA), la tecnología del aparato administrativo estatal (y una especial sensibilidad en contra del manejo de ella por parte del Estado a partir de las experiencias provenientes del nacionalsocialismo) y la denominada seguridad del Estado (en la RFA, la Policía estatal y el Servicio de Seguridad del Estado fundamentaban, mediante la vigilancia de los ciudadanos y la recolección de datos, las operaciones policíacas), constituyeron los importantes antecedentes tributarios de la configuración del derecho a la autodeterminación informativa⁸¹.

No podemos omitir poner de manifiesto que, en lo expuesto en el párrafo anterior, percibimos una indisimulada coincidencia con los aciagos momentos vividos en Argentina durante la última dictadura militar (1976-1983): el acopio de información por parte del Estado, la alegada seguridad nacional y la imperiosa necesidad de abrir los archivos de los organismos de seguridad estatales para conocer la realidad acerca de la enorme cantidad de personas desaparecidas. Al respecto, los casos "Suárez Mason" y "Urteaga" de la Corte Suprema de Justicia argentina, con soluciones dicotómicas, testimonian que el hábeas data puede funcionar como medio para levantar la barrera que obstaculiza proporcionar tal información y, de ese modo, operativizar el derecho de autodeterminación informativa. La doctrina sentada por dicho Tribunal adquiría plusvalía pues ambos pronunciamientos fueron emitidos con anterioridad al dictado de la ley reglamentaria del hábeas data contenido en el ya referido párrafo 3° del artículo 43 constitucional.

Lo anticipado nos tiende el puente hacia la reseña que de ambos fallos realizaremos a continuación⁸², en los que –finalmente– se discutían diversos aspectos conectados con el hábeas data.

En la causa *Suárez Mason*⁸³ (fallada el 13 de agosto de 1998), la Corte tuvo ocasión de resolver el recurso extraordinario interpuesto por la Sra. Aguiar de Lapacó (madre de una persona desaparecida) contra la resolución de la Cámara Na-

burstag, a cargo de HORN, N. y BECK, C. H., München, 1982, pp. 513 y ss.; aludido por PÉREZ LUÑO, ANTONIO-ENRIQUE, ídem nota anterior.

⁸⁰ En HASSEMER, WINFRIED y CHIRINO SÁNCHEZ, ALFREDO, *El derecho a la autodeterminación informativa y los retos del procesamiento automatizado de datos personales*, Editores del Puerto, Buenos Aires, Argentina, 1997, p. 28.

⁸¹ *Ibíd.*, pp. 29/32.

⁸² A título informativo, debe recordarse que desde el dictado de las mismas se han producido numerosos cambios en la integración del Máximo Tribunal argentino.

Así, se concretaron las renunciaciones de los doctores Bossert y Nazareno, quienes fueron reemplazados, respectivamente, por los ministros Maqueda y Zaffaroni. Tampoco están ya los doctores López y Moliné O'Connor. Una de tales vacantes fue cubierta por la doctora Highton de Nolasco y la restante, por la doctora Argibay. Igualmente, ha dimitido el doctor Vázquez y se ha incorporado el doctor Lorenzetti. Por último, en fecha reciente también ha renunciado el doctor Belluscio.

En consecuencia, el tribunal ha quedado integrado con los siguientes ministros: Petracchi (presidente), Argibay, Fayt, Boggiano (cuyo juicio político está en trámite ante el Congreso de la Nación), Maqueda, Zaffaroni, Highton de Nolasco y Lorenzetti. En otras palabras, cuenta con ocho (8) de los nueve (9) miembros fijados legalmente.

⁸³ El fallo puede ser consultado en *La Ley*, T° 1998-E, Buenos Aires, Argentina, pp. 215 y ss.

cional de Apelaciones en lo Criminal y Correccional Federal que había decidido – por mayoría– tener presente la respuesta producida por el Estado Mayor del Ejército relativa al destino de las personas desaparecidas en la jurisdicción dependiente del Primer Cuerpo del Ejército entre los años 1976 y 1983, ordenando la prosecución de la causa según su estado, lo que entrañaba una denegatoria de diversas medidas de prueba impetradas en la causa.

En un tan escueto como oscuro fallo, la mayoría de la Corte (votos de los doctores Nazareno, Moliné O'Connor, Belluscio, López y Vázquez) decidió declarar improcedente el recurso extraordinario incoado en virtud de que, a su criterio, no resultaba admisible la realización de diligencias investigativas que tenían por finalidad comprobar la existencia de un hecho punible y descubrir a los autores, pues en el estado en que el caso se encontraba al momento de fallar, su objeto procesal había quedado agotado, razón por la cual la concreción de tales medidas hubiese implicado la reapertura del proceso contra quienes habían sido sobreseídos definitivamente por los hechos que dieron lugar a la formación de la causa.

El pronunciamiento recibió las disidencias conjunta de los doctores Petracchi y Bossert e individuales de los ministros Fayt y Boggiano, quienes coincidieron en cuanto a la procedencia del recurso extraordinario y la consecuente revocación del fallo puesto en crisis.

De las anunciadas disidencias, sólo nos detendremos en la impulsada por el doctor Boggiano, quien aportó algunas consideraciones interesantes en cuanto al tema alrededor del cual gira el presente trabajo, pues aludió a la acción de hábeas data contenida en el art. 43, párrafo 3º, de la Constitución Nacional (CN). Sintéticamente, sostuvo:

- Que en virtud del principio *iura novit curia*, incumbe a la Corte calificar la verdadera índole jurídica de la cuestión ventilada, su fundamento y trascendencia, con mayor razón cuando –como en el caso– estaba en juego una norma de la Ley Fundamental; principio del que desprende la siguiente conclusión: en autos la recurrente no había solicitado sino su derecho a conocer los datos existentes en registros o bancos de datos públicos (art. 43, párrafo 3º, CN), habiendo sido despojada de ese derecho por parte de la Cámara *a quo* (considerando 7º). Respecto de tal conclusión del doctor Boggiano, no sin cautela, Morello ha sostenido que: “Poniendo entre paréntesis si esa facultad-deber pudo ejercerse oficiosamente con la profundidad de acordar virtualidad a una acción que no había sido propuesta por la peticionaria, coincidimos en que la amplitud de la garantía del ‘hábeas data’ facultaba a su uso propio por la solicitante, legitimada para poder acceder a una información personal que de manera tan directa le concernía”⁸⁴;

- evocando la doctrina que la Corte sentara en “*Siri*”⁸⁵, el ministro Boggiano afirmó que quedaba claro que la operatividad de una norma constitucional no depende de ley alguna que la reglamente (considerando 8º);

⁸⁴ MORELLO, AUGUSTO M. “Los contenidos de la pretensión procesal penal y de la garantía de «hábeas data»”, *La Ley*, Tº 1998-F, Buenos Aires, Argentina, p. 369.

⁸⁵ *Fallos*, 239:459.

Se trata de un célebre caso –resuelto el 27 de diciembre de 1957– en el que la Corte Suprema de Justicia argentina, por mayoría, creó pretorianamente la figura del amparo contra actos de autoridad pública, luego de que durante décadas negara la existencia del mismo sustentándose en que el legislador no había instituido tal tipología de procesos.

- que en el art. 43, párrafo 3º, la “Constitución ha incorporado un nuevo derecho a la protección de los datos personales frente a cualquier intromisión arbitraria o abusiva que pudiera implicar una violación a la intimidad y a los demás derechos constitucionales” (considerando 10), además de consagrar una garantía para que el titular pueda conocer y controlar los datos referentes a su persona que obren en registros públicos o privados destinados a proveer informes para que, en caso de falsedad o inexactitud, pueda exigir la supresión, confidencialidad o actualización cuando ellos afecten derechos consagrados en la CN (considerando 11);

- es insuficiente concebir el derecho a la intimidad como un derecho destinado a excluir a los terceros de la zona de reserva, sin contar al propio tiempo con un derecho de control sobre el flujo de informaciones que conciernen a cada sujeto (considerando 13); y

- que de acuerdo con el citado art. 43, párrafo 3º, la actora estaba suficientemente legitimada pues se había afectado su ámbito de intimidad; por tal razón, entendió el magistrado votante que una interpretación inadecuada frustraría la verdadera razón de dicha norma y “tornaría la garantía escrita en mera retórica vacía de fuerza jurídica” (considerando 15).

Por su parte, cabe recordar que *in re* “U. 14. XXXIII. - Urteaga, Facundo Raúl c/ Estado Nacional - Estado Mayor Conjunto de las FF.AA. s/ amparo ley 16.986”, resuelto por la Corte Suprema de Justicia de la Nación el 15 de octubre de 1998, las instancias de mérito habían coincidido en cuanto al rechazo de la “acción de amparo de hábeas data” (*sic*) que el peticionante articulara contra el Estado Nacional y/o el Estado Mayor Conjunto de las Fuerzas Armadas y/o el Gobierno de la Provincia de Buenos Aires, destinada a “obtener información que exista en los Bancos de Datos de la Secretaría de Informaciones del Estado, Servicio de Inteligencia del Ejército, Servicio de Informaciones de la Armada, Servicios de Informaciones de la Aeronáutica, Servicio de Inteligencia de la Policía Federal, Servicio de Informaciones de la Policía de la Provincia de Buenos Aires y Servicio de Inteligencia de la Provincia de Buenos Aires y/o cualquier otro del Estado Nacional, de las Fuerzas Armadas y del Gobierno de la Provincia de Buenos Aires, sobre su hermano Benito J. Urteaga, supuestamente ‘abatido’ el 19 de julio de 1976 en un departamento ubicado en la localidad de Villa Martelli, Partido de Vicente López, Provincia de Buenos Aires...”⁸⁶.

Si bien todos los magistrados coincidieron en la solución final implementada, consistente en hacer lugar al recurso extraordinario y revocar la sentencia puesta en crisis, se torna un poco complicado rearmar uniformemente la estructura del fallo emitido, en virtud de que los diversos votos presentan tanto similitudes cuanto discrepancias.

Por tanto, y para escapar de tal complejidad, sólo diremos que en lo concerniente a la *ruta procesal* escogida por el actor, los magistrados Nazareno, Moliné O’Connor, Boggiano, Petracchi y Vázquez juzgaron que la acción de hábeas data era la adecuada. Por su parte, los doctores Belluscio y López (en voto conjunto) y Fayt y Bossert (individualmente) sostuvieron que la vía procedente era la del am-

⁸⁶ La transcripción fue tomada del considerando 2º del fallo de la Corte; *La Ley*, *loc. cit.* en nota 84, p. 237.

paro, bien que advirtiendo los dos magistrados citados en último término, que el hábeas data es una forma de amparo⁸⁷.

El detalle de los votos emitidos fue el siguiente: los doctores Nazareno y Moliné O'Connor, se expidieron conjuntamente; los ministros Belluscio y López, también lo hicieron en conjunto; y los magistrados Fayt, Petracchi, Boggiano, Bossert y Vázquez plasmaron sus votos individualmente.

Veamos, sintéticamente, qué dijeron:

Los doctores Nazareno y Moliné O'Connor, de quienes podría decirse constituyeron “la mayoría”, recordaron la doctrina de la Corte por virtud de la cual la falta de reglamentación legislativa no empuja a la vigencia de ciertos derechos que, por su índole, “pueden ser invocados, ejercidos y amparados sin el complemento de disposición legislativa alguna” (considerando 9°), marco de ausencia reglamentaria en el que juzgaban correspondía a la Corte delinear –con flexibilidad razonable– los alcances de la acción de hábeas data, en orden a conferir al requirente la plena protección que ella establece (considerando 12), debiendo admitirse la legitimación de éste, toda vez que –en su calidad de hermano de la persona supuestamente fallecida– “la habilitación para accionar de un familiar directo con sustento en el derecho a que se proporcione información, aparece, en las circunstancias del caso, como una de las alternativas de reglamentación posibles en el marco de una discreta interpretación del texto constitucional” (considerando 13). Concluyeron sosteniendo que correspondía reconocer al recurrente el derecho a la información objetiva requerida (considerando 15). Apoyándose en las directrices formuladas por la ONU, la OEA, el Consejo de Europa y la jurisprudencia de la Corte Europea de Derechos Humanos, entendieron que la amplitud de los alcances de la acción de hábeas data, tanto en lo relativo a la exigencia de licitud, lealtad y exactitud en la información, como lo concerniente al acceso de los sujetos legitimados “encuentra limitaciones, fundamentalmente, en razones de seguridad y defensa nacional” (considerando 11); argumento que veremos reproducido en “Ganora” (considerando 9°, sobre el que volveremos).

- Los magistrados Belluscio y López sostuvieron que el planteo del actor no guardaba relación con la garantía protegida mediante el hábeas data (considerando 6°) sino que tal planteamiento debía ser ubicado en el marco del amparo en general (considerando 7°), siendo admisible su pretensión “cualquiera que sea el *nomen iuris* adoptado para ser concedido” (considerando 12), pasando a reconocer al peticionario el derecho a la información objetiva exigida (considerando 13).

- El doctor Fayt arribó a idéntica conclusión que los magistrados Belluscio y López, entendiendo que entre el planteo que se efectivizaba en autos y la garantía de hábeas data existían claras diferencias, pues aquél “no es otra cosa que el reclamo a los jueces –en tanto guardianes de las garantías individuales– para que hagan valer lo establecido en los arts. 14 y 32 CN⁸⁸: esto es, el derecho a la información que es preexistente a la incorporación del hábeas data en nuestra Ley Fundamental” (considerando 11), para pasar a puntualizar que era la genérica acción de amparo el medio eficaz para que el solicitante obtuviera de los poderes públicos y sus

⁸⁷ Cfr. BIANCHI, ALBERTO B. “El hábeas data como medio de protección del derecho a la información objetiva en un valioso fallo de la Corte Suprema”, *La Ley*, loc. cit. en nota 84, p. 299.

⁸⁸ Ambas normas se refieren a la libertad de expresión, contentiva del derecho a la información.

organismos de seguridad las respuestas encaminadas a conocer los antecedentes que pudieran existir acerca de la situación de su hermano (*idem*);

- a su turno, el ministro Bossert expresó que el derecho a ser informado acerca del hermano desaparecido del peticionante, y supuestamente muerto, constituía uno de los derechos esenciales del hombre contenidos en el art. 33 CN⁸⁹ (considerando 19), añadiendo que el *nomen iuris* de la vía procesal intentada por el accionante no ataba al juez, quien debía analizar los hechos, la pretensión articulada y el derecho aplicable con prescindencia de las calificaciones que las partes hicieran, ello en virtud del principio *iura novit curia* (considerando 22); además, indicó que el párrafo 3° del art. 43 CN deja entrever que se trata de una forma específica de la acción de amparo establecida en términos genéricos en el párrafo 1° de dicha norma, por lo que el supuesto diagramado en el 3° no agota ni excluye otras posibilidades de indagación de datos asentados en registros públicos o privados mediante la acción de amparo del párrafo 1° (*idem*);

- en un interesante voto, el doctor Petracchi sostuvo que lo solicitado por el recurrente se encontraba amparado por el art. 43, párrafo 3°, CN, “sin que exista óbice formal alguno para garantizar la procedencia del hábeas data intentado por la vía de la norma citada” (considerando 17), luego de sustentarse en la “autodeterminación informativa” (considerando 10) y de reseñar las palabras del Tribunal Constitucional Federal alemán en la sentencia sobre la Ley del Censo: “si un ciudadano no tiene información sobre quién ha obtenido información sobre él, qué tipo de información y con qué medios la ha obtenido, ya no podrá participar en la vida pública sin miedo” (*vid.* considerando 11 del voto del doctor Petracchi);

- en un muy breve voto, el doctor Boggiano indicó con claridad —luego de dejar sentado en el considerando 1° que la cuestión debatida en autos era sustancialmente análoga a la examinada en “Suárez Mason” y sustentarse, ya en el considerando 2°, en la doctrina de la Corte dimanante del caso “Kot”⁹⁰— que “el derecho de hábeas data puede hacerse valer por cualquier vía procesal razonable, aun incidental, hasta tanto una ley reglamente su ejercicio” (considerando 3°); y

- por fin, el doctor Vázquez manifestó que, cuando el art. 43 legisla sobre el hábeas data, al igual que cuando se refiere al amparo y al hábeas corpus, lo hace a través de una norma de carácter operativo, es decir, aquella que está dirigida a una situación de la realidad sobre la que pueda operar inmediatamente, o sea, sin necesidad de instituciones que deban ser establecidas por el Congreso (considerando 5°), incumbiendo —en situaciones como la de autos— a los órganos jurisdiccionales determinar en forma provisoria las características con que tal derecho habría de desarrollarse en los casos concretos, hasta tanto el Congreso procediera a su determinación definitiva (*idem*). Concluyó asegurando que el actor se encontraba legitimado para interponer la acción de hábeas data para obtener datos que no eran propios, dado que se trataba de un miembro del grupo familiar directo con interés legítimo, además de que el sujeto legitimado activamente estaba imposibilitado de ejercer la mentada acción (considerando 8°).

⁸⁹ Dicho precepto alude a los derechos implícitos.

⁹⁰ Fallos, 241:291.

Profundizando la línea abierta en el citado caso “Siri”, en “Kot” (dirimido el 5 de setiembre de 1958), la Corte Suprema de Justicia argentina —por mayoría— gestó jurisprudencialmente el amparo contra actos de particulares, aun cuando se declarara que el mismo se extraía del art. 33 CN como derecho o garantía no enumerado.

Del empalme de ambos casos, puede observarse que la solución impresa a “Urteaga” reviste trascendencia en tanto la Corte argentina se expidió en favor de la virtualidad del hábeas data para requerir información acerca del destino de una persona desaparecida, supuestamente ultimada en un enfrentamiento con las fuerzas armadas o de seguridad de la Provincia de Buenos Aires, solución complementada por el mismo Tribunal en un caso posterior: “G. 529. XXXIII. - *Ganora, Marlo Fernando y otra s/ hábeas corpus*”, dirimido el 16 de setiembre de 1999, en el que se resolvió que, en principio, la obtención de información sobre datos de carácter personal obrantes en organismos y fuerzas de seguridad encuentra adecuación legal en la acción de hábeas data, sin perjuicio de que el suministro de tal información pudiera, eventualmente, afectar la seguridad, la defensa nacional, las relaciones exteriores o una investigación criminal, cuestión que en cada caso debería ser invocada por el titular de la institución requerida y, desde nuestro punto de vista, meritada por la autoridad judicial interviniente para determinar si media un interés público relevante para restringir el derecho de autodeterminación informativa o si, por el contrario, no concurre en el particular la trascendencia exigible para relevar al organismo de su obligación de informar.

Tangencialmente, y para corroborar que lo resuelto en “*Ganora*” sobre la legitimación pasiva de, *inter alia*, los organismos de seguridad del Estado no constituye una ocurrencia *esotérica* de la Corte, corresponde indicar que la Ley N° 25.326 (dictada con posterioridad a tal decisorio), dispone que quedan sujetos a dicho régimen legal los datos personales que, por haberse almacenado para fines administrativos, deban ser objeto de registro permanente en los bancos de datos de las fuerzas armadas, de seguridad, organismos policiales o de inteligencia (art. 23.1). Asimismo, preceptúa que el tratamiento de datos personales con fines de defensa nacional o seguridad pública por parte de los organismos mencionados, sin consentimiento de los afectados⁹¹, queda limitado a aquellos supuestos y categoría de datos que resulten necesarios para el estricto cumplimiento de las misiones legalmente asignadas a aquéllos para la defensa nacional, la seguridad pública o la represión de los delitos (art. 23.2).

En definitiva, y previo a dar paso a las consideraciones finales del presente trabajo, vemos que el fallo emitido en “Urteaga” –que habría visto la luz luego de haber sido concebido al influjo de la negativa crítica que despertara el criterio sentado por el Tribunal en “Suárez Mason” (que incluso originó una denuncia contra el Estado argentino ante la Comisión Interamericana de Derechos Humanos)–, también resulta importante toda vez que la Corte ha dado un laudable paso adelante en pro del ensanchamiento de la legitimación procesal activa, al estimar procedente la acción de hábeas data incoada por quien no perseguía el derecho a informarse respecto de datos propios, sino de los de un hermano eventualmente fallecido, trasladándose así el potencial ejercicio de la acción a un familiar directo del afectado. Asimismo, resulta plausible que en el mencionado pronunciamiento se haya reiterado el valioso criterio hermenéutico que sostiene la innecesariedad de la existen-

⁹¹ Respecto de la captación de datos personales sin el consentimiento de la persona concernida y la necesidad de establecer una protección adicional para compensar preventivamente tal falta de consentimiento inicial, ver BAZÁN, VÍCTOR, “Hábeas data, registros de cumplimiento o incumplimiento de obligaciones patrimoniales, y saneamiento del crédito: la copa medio llena o medio vacía”, *La Ley, Suplemento de Derecho Constitucional*, Buenos Aires, Argentina, 29 de noviembre de 1999, pp. 1/11, en esp. pp. 5/7.

cia de ley reglamentaria cuando de viabilizar el ejercicio de un derecho o de una garantía deparados constitucionalmente se trata.

EPÍLOGO

Del recorrido analítico precedente, pueden extraerse las siguientes ideas de cierre:

1. Para una regulación integral del instituto del hábeas data y demás cuestiones vinculadas con éste y, paralelamente, una prefiguración del contenido mínimo del derecho de autodeterminación informativa, la normativa que se pretenda implementar para captar la integralidad de la cuestión, no debería soslayar los siguientes extremos (enunciados ilustrativamente), debiendo además precisarse claramente las excepciones a la procedencia de aquel proceso:

- Que la recolección de datos personales sea efectuada por medios lícitos.
- Que la información personal recogida sea utilizada para el fin (lícito) con el que se recolectó.
- Que el tratamiento de los datos personales, además de necesario, sea adecuado, es decir, razonable *vis-à-vis* el fin perseguido.
- Que se garantice la calidad de la información personal obrante en el fichero, registro, archivo, base o banco de datos (de acuerdo con la nomenclatura que se seleccione), o sometida a tratamiento.
- Que se limite el tratamiento de información personal intrínsecamente sensible susceptible de generar una discriminación ilegítima o arbitraria.
- Que los datos personales sean conservados durante el tiempo realmente necesario para el cumplimiento del objetivo para el que fueron captados.
- Que se adopten las medidas tuitivas indispensables para evitar el acceso no autorizado, la modificación, la revelación o la destrucción (aun accidental) de los datos personales.
- Que pueda identificarse fácilmente al titular del fichero, registro, archivo, base o banco de datos, a fin de poder –potencialmente– asignarle responsabilidad –*inter alia*– por el incumplimiento de las obligaciones a su cargo o por su accionar lesivo.

- Que se diseñen pautas procedimentales y procesales adecuadas que permitan al interesado legitimado ejercer el derecho de acceso a la información personal contenida en el fichero, registro, archivo, base o banco de datos y, subsiguientemente, el de intervención sobre dicha información, es decir, por caso, que se operativice la facultad de rectificarla, suprimirla o someterla a confidencialidad.

2. El concepto preinformático de la *intimidación* deviene inoperante frente a la actual ebullición tecnológica. De cualquier modo, la obsolescencia conceptual no puede ser pretexto para consentir la desprotección sustancial del derecho a que refiere el enunciado lingüístico⁹².

⁹² No es irrelevante la posición de FROSINI, cuando suministra su visión en relación con los derechos humanos en la era tecnológica, particularizando respecto del *right to privacy*, al que juzga no ya sólo como el derecho a la protección de la esfera personal de la intimidad, sino también como comprensivo de la posibilidad de disponer en forma libre del derecho a la propia imagen informática y, por ende, de conocer los datos personales que sean registrados y electrónicamente procesados por particulares o por la propia Administración (FROSINI,

En ese sentido, el derecho de autodeterminación informativa ofrece una textura que resulta acorde con los modernos desafíos informáticos⁹³, pues justamente permite abandonar el concepto de intimidad como libertad negativa y avanzar hacia una fase *activa* del proceso de circulación de la información personal brindando protagonismo al interesado⁹⁴ y posibilitándole el ejercicio del “control que a cada uno de nosotros nos corresponde sobre la información que nos concierne personalmente, sea íntima o no, para preservar, de este modo y en último extremo, la propia identidad, nuestra dignidad y libertad”, tal como expone LUCAS MURILLO DE LA CUEVA⁹⁵.

No se trata solamente del control de la información personal respecto de su divulgación a terceros, sino también, sobre el uso posterior de aquella una vez que ha sido facilitada, es decir, el derecho a “perseguir” los datos personales, a conocer el camino que seguirán para vigilar la utilización correcta y lícita de los mismos en relación con los fines para los que se obtuvieron⁹⁶. En otras palabras, dicho derecho no sólo adquiere validez para el almacenamiento de los datos, sino también a lo largo de todo el proceso de obtención de la información, de tal manera que la forma de almacenamiento de los datos (manual o electrónica) no ostenta un verdadero papel fundamental⁹⁷.

Es que, como lo manifestara la reiteradamente aludida sentencia del Tribunal Constitucional alemán sobre la Ley del Censo de Población, “no serían compatibles con el derecho a la autodeterminación informativa un orden social y un orden jurídico que hiciese posible al primero, en el que el ciudadano ya no pudiera saber quién, qué, cuándo y con qué motivo sabe sobre él”.

Como acertadamente afirma HERRÁN ORTIZ, la vida privada, la propia imagen, la igualdad del ser humano, su libre desarrollo personal, y el pleno ejercicio de sus derechos constituyen bienes jurídicos personales cuya salvaguarda se debe procurar mediante el sistema de protección de datos. Así, sólo ocasionalmente esta última garantizará la intimidad del individuo entendida como ámbito esencial e interior del ser humano, y ello, por cuanto esa información trascendente del individuo no supera el ámbito interior de la persona⁹⁸. Añade la autora citada que la realidad demuestra que lo verdaderamente tutelado a través del derecho de autodeterminación

VITTORIO, “Los derechos humanos en la era tecnológica”, en el libro colectivo coordinado por PÉREZ LUÑO, ANTONIO-ENRIQUE, *Derechos humanos y constitucionalismo ante el tercer milenio*, Marcial Pons, Madrid, España, 1996, p. 94.

⁹³ Ver para ampliar, BAZÁN, VÍCTOR, “Sobre la cobertura tuitiva del hábeas data (especial referencia al derecho federal argentino)”, *Revista del Foro*, N° 2, Año LXXXVI, Colegio de Abogados, Lima, Perú, 1998, pp. 143/151.

⁹⁴ Tangencialmente, diremos con CASCAJO CASTRO que la génesis de la LORTAD (hoy derogada) se sitúa en la tendencia al pasaje de “la delimitación conceptual del derecho a la intimidad desde la facultad de aislamiento al poder de control sobre las informaciones que son relevantes para cada sujeto” (CASCAJO CASTRO, JOSÉ LUIS, “Tratamiento automatizado de los datos de carácter personal”, *Problemas actuales de los derechos fundamentales*, Edición de José María Sauca, ‘I Seminario Internacional sobre Problemas Actuales de los Derechos Fundamentales’, Instituto Universitario de Derechos Humanos ‘Bartolomé de las Casas’, Universidad Carlos III - BOE, Madrid, España, 1994, p. 365).

⁹⁵ LUCAS MURILLO DE LA CUEVA, PABLO, *op. cit.* “Informática y protección...”, pp. 32/33.

⁹⁶ Cfr. HERRÁN ORTIZ, ANA ISABEL, *La violación de la intimidad en la protección de datos personales*, Dykinson, Madrid, España, 1999, pp. 91/92.

⁹⁷ CHIRINO SÁNCHEZ, ALFREDO, *op. cit.*, p. 104.

⁹⁸ HERRÁN ORTIZ, ANA ISABEL, *op. cit.*, p. 367.

ción informativa son comportamientos, experiencias, conductas de la persona que la descubren ante los demás y que, sin calificarse de íntimos o secretos, el individuo no desea compartir, y menos aún, que queden registrados para un posterior tratamiento automatizado, dado que ello significaría tanto como despojarse de su identidad e individualidad ante los demás, peligrando incluso el libre desarrollo de su personalidad⁹⁹.

Aquel derecho autodeterminativo resulta útil como coadyuvante de la necesaria superación del preconcepto que indica que el binomio informática-intimidación está inextricablemente unido, pues aun cuando ambos elementos guarden conexión, tal visión termina por opacar el meollo del problema y conduce a una confusión entre el fenómeno y su premisa, desde que, por ejemplo, la lesión a la intimidad puede funcionar como antecedente previo para el ulterior tratamiento ilegítimo de la información personal recogida. No habrá que perder de vista que existen datos sensibles que, aun cuando no íntimos, claman por protección jurídica¹⁰⁰.

3. La necesidad de establecer jurídicamente medidas de protección de los datos personales frente a la informatización, se debe no tanto al carácter privado que algunos de ellos puedan tener, sino a las múltiples posibilidades de elaboración e interrelación propias de la tecnología informática, pues como ha sostenido el Tribunal Constitucional Federal alemán en el señalado pronunciamiento, “un dato carente en sí mismo de interés puede cobrar un nuevo valor de referencia y, en esta medida, ya no existe, bajo las condiciones de la elaboración automática de datos, ninguno «sin interés»”¹⁰¹.

Es que existen datos en apariencia inocuos o irrelevantes que, de modo súbito, se convierten en extremadamente sensibles mediante un sencillo cambio del fin que se persiguiera al momento de su recolección. No deja de ser relevante procurar evitar las consecuencias perniciosas de la *inferential relation retrieval*, que consiste en la descontextualización de la información a través del “cruce” de datos veraces con otras referencias de signo distinto, lo que arroja como precipitado una información no cabal¹⁰², en cuyo caso la agresión a la autodeterminación informativa se produce, no ya porque se genere una apropiación incontrolada de los mismos, “sino porque se instrumentalizan los disponibles para fabricar una personalidad y sustituir la propia identidad por otra que no tiene por qué corresponderse con la verdadera”¹⁰³.

Como aprecia OROZCO PARDO¹⁰⁴, que un dato es inocuo o sensible, no ya por su contenido, sino por el uso que de él se haga. Por tanto, preliminarmente, sólo indicaremos que el énfasis debe ser puesto en el fin para el que se emplea la información colectada, por lo que las garantías tuitivas del derecho de autodeterminación informativa deberían focalizar la utilización que de la información se haga, y no tanto la calificación apriorística de si un dato es sensible o no lo es¹⁰⁵.

⁹⁹ *Ibid.*, pp. 367/368.

¹⁰⁰ Vid. JIMÉNEZ ESCOBAR, R., *op. cit.*, pp. 242/243.

¹⁰¹ LUCAS MURILLO DE LA CUEVA, PABLO, *op. cit. El derecho a la autodeterminación informativa*, p. 122.

¹⁰² *Ibid.*, p. 111.

¹⁰³ LUCAS MURILLO DE LA CUEVA, PABLO, *op. cit.* “Informática y protección...”, p. 83.

¹⁰⁴ OROZCO PARDO, GUILLERMO, *op. cit.*, p. 222.

¹⁰⁵ Cftar. PÉREZ LUÑO, ANTONIO-ENRIQUE, ‘III Congreso Iberoamericano de Informática y Derecho’, Coloquios, Mesa N° 2, *cit.*, *Informática y Derecho*, N° 5, p. 364.

4. El de autodeterminación informativa es un derecho autónomo, con una doble dimensión: sustancial, como derecho en sí mismo; e instrumental, es decir, como soporte para la cobertura tutelar de otros derechos, *inter alia*, de los de intimidad, honor y dignidad.

Se trata de un derecho a saber y también un derecho a la transparencia del procesamiento de datos, el cual a su vez es una parte fundamental del concepto moderno de democracia¹⁰⁶.

5. El aludido derecho es, precisamente por su condición de tal, relativo. El límite que se erige frente a su despliegue vivencial viene marcado por el innegable valor que asume la información como bien colectivo en el conjunto social. Asimismo, no debería soslayarse la necesidad de imponer un tratamiento democrático de la información, procurando unir los esfuerzos (públicos y privados) para lograr un sano equilibrio axiológico de los bienes en juego interactivo.

En la dirección apuntada, y nutriéndonos de las enseñanzas de PÉREZ LUÑO, sería una necesidad olvidar que el Estado de Derecho requiere para su adecuado funcionamiento de un conjunto de informaciones, pues la planificación económica, la prevención sanitaria, la política fiscal, la lucha contra las actividades delictivas, etc., serían impensables sin el soporte de un completo y eficaz aparato informático; sin embargo, de una obcecación no menor sería soslayar la importancia del establecimiento de límites que, sin impedir el acopio de información por parte del Estado, concomitantemente garanticen los derechos fundamentales de sus habitantes (PÉREZ LUÑO ciñe tal objetivo a la protección de los “ciudadanos”), configurando un equilibrio de poderes y situaciones que se torna indispensable para una sana pervivencia de la comunidad democrática¹⁰⁷.

En íntima conexión con lo expuesto, y siguiendo una vez más a PÉREZ LUÑO, no se trata de impedir el proceso electrónico de informaciones necesarias para el funcionamiento de cualquier Estado moderno, sino de asegurar un uso democrático de la tecnología de la información¹⁰⁸.

Obviamente, habrá de tenerse presente que la premisa es (como lo sostuvo la “Comisión de Informática y Libertades” francesa) dominar, y no paralizar la informática. En todo caso, deberán canalizarse los esfuerzos para evitar que el avance técnico y científico se configure a cualquier costo, pues sería lamentable que la evolución tecnológica aparejara una consecuente involución cualitativa de la protección de los derechos fundamentales.

En línea con ello, se ha precisado que el Derecho no sale indemne de su confrontación con la técnica¹⁰⁹. En tal espacio de vinculación, el hábeas data se encarama como valioso instrumento preventivo o correctivo de las disfuncionalidades que de aquella pudieran originarse, particularmente, en el arco de tensiones derivables de la coexistencia de los derechos fundamentales y el vertiginoso desarrollo tecnológico-informático.

¹⁰⁶ CHIRINO SÁNCHEZ, ALFREDO, *op. cit.*, p. 104.

¹⁰⁷ PÉREZ LUÑO, ANTONIO-ENRIQUE, “Dilemas actuales de la protección de la intimidad”, *loc. cit.* en nota 94, *Problemas actuales de los...*, p. 322.

¹⁰⁸ Paráfrasis de la afirmación de PÉREZ LUÑO, ANTONIO-ENRIQUE, “La protección de la intimidad frente a la informática en la Constitución española de 1978”, *REP*, mayo-junio de 1979, p. 68.

¹⁰⁹ CIFUENTES MUÑOZ, EDUARDO, *op. cit.*, p. 117.